

EXHIBIT 22-2

[Home](#) / [Publications](#) / [High-risk and other monitored jurisdictions](#)/ [Public Statement - 24 October 2014](#)

Public Statement - 24 October 2014

[Send](#)[Print](#)[Tweet](#)

FATF Public Statement: 24 October 2014

[Download pdf \(428kb\)](#)

Paris, 24 October 2014 - The Financial Action Task Force (FATF) is the global standard setting body for anti-money laundering and combating the financing of terrorism (AML/CFT). In order to protect the international financial system from money laundering and financing of terrorism (ML/FT) risks and to encourage greater compliance with the AML/CFT standards, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.

Jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/FT) risks emanating from the jurisdictions.

[Iran](#)[Democratic People's Republic of Korea \(DPRK\)](#)

Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction, as described below.

[Algeria](#)[Ecuador](#)[Indonesia](#)[Myanmar](#)

Iran

The FATF remains particularly and exceptionally concerned about Iran's failure to address the risk of terrorist financing and the serious threat this poses to the integrity of the international financial system, despite Iran's previous engagement with the FATF and recent submission of information.

The FATF reaffirms its call on members and urges all jurisdictions to advise their financial institutions to give special attention to business relationships and transactions with Iran, including Iranian companies and financial institutions. In addition to enhanced scrutiny, the FATF reaffirms its 25 February 2009 call on its members and urges all jurisdictions to apply effective counter-measures to protect their financial sectors from money laundering and financing of terrorism (ML/FT) risks emanating from Iran. The FATF continues to urge jurisdictions to protect against correspondent relationships being used to bypass or evade counter-measures and risk mitigation practices and to take into account ML/FT risks when considering requests by Iranian financial institutions to open branches and subsidiaries in their jurisdiction. Due to the continuing terrorist financing threat emanating from Iran, jurisdictions should consider the steps already taken and possible additional safeguards or strengthen existing ones.

The FATF urges Iran to immediately and meaningfully address its AML/CFT deficiencies, in particular by criminalising terrorist financing and effectively implementing suspicious transaction reporting requirements. If Iran fails to take concrete steps to continue to improve its CFT regime, the FATF will consider calling on its members and urging all jurisdictions to strengthen counter-measures in February 2015.

Democratic People's Republic of Korea (DPRK)

Since June 2014, the DPRK has further engaged directly with the FATF and APG to discuss its AML/CFT deficiencies. The FATF urges the DPRK to continue its cooperation with the FATF and to provide a high-level political commitment to the action plan developed with the FATF.

The FATF remains concerned by the DPRK's failure to address the significant deficiencies in its anti-money laundering and combating the financing of terrorism (AML/CFT) regime and the serious threat this poses to the integrity of the international financial system. The FATF urges the DPRK to immediately and meaningfully address its AML/CFT deficiencies.

The FATF reaffirms its 25 February 2011 call on its members and urges all jurisdictions to advise their financial institutions to give special attention to business relationships and transactions with the DPRK, including DPRK companies and financial institutions. In addition to enhanced scrutiny, the FATF further calls on its members and urges all jurisdictions to apply effective counter-measures to protect their financial sectors from money laundering and financing of terrorism (ML/FT) risks emanating from the DPRK. Jurisdictions should also protect against correspondent relationships being used to bypass or

evade counter-measures and risk mitigation practices, and take into account ML/FT risks when considering requests by DPRK financial institutions to open branches and subsidiaries in their jurisdiction.

Algeria

Algeria has taken steps towards improving its AML/CFT regime. However, despite Algeria's high-level political commitment to work with the FATF and MENAFATF to address its strategic AML/CFT deficiencies, Algeria has not made sufficient progress in implementing its action plan within the established timelines, and certain strategic deficiencies remain. Algeria should continue to work on implementing its action plan to address these deficiencies, including by: (1) adequately criminalising terrorist financing; (2) establishing and implementing an adequate legal framework for identifying, tracing and freezing terrorist assets and (3) adopting customer due diligence obligations in compliance with the FATF Standards. The FATF encourages Algeria to address its remaining deficiencies and continue the process of implementing its action plan.

Ecuador

Ecuador has taken steps towards improving its AML/CFT regime including by issuing AML/CFT regulations for companies supervised by Superintendence of Companies. However, despite Ecuador's high-level political commitment to work with the FATF and GAFISUD to address its strategic AML/CFT deficiencies, Ecuador has not made sufficient progress in implementing its action plan, and certain strategic deficiencies remain. Ecuador should continue to work on implementing its action plan to address these deficiencies, including by (1) establishing and implementing adequate procedures to identify and freeze terrorist assets and (2) clarifying procedures for the confiscation of funds related to money laundering. Ecuador should also continue enhancing financial sector supervision. The FATF encourages Ecuador to address its remaining deficiencies and continue the process of implementing its action plan.

Indonesia

Indonesia has taken steps towards improving its AML/CFT regime including by further implementing its terrorist asset-freezing regime. However, despite Indonesia's high-level political commitment to work with the FATF and APG to address its strategic CFT deficiencies, Indonesia has not made sufficient progress in implementing its action plan within the agreed timelines, and certain key CFT deficiencies remain regarding the development and implementation of an adequate legal framework and procedures for identifying and freezing of terrorist assets. The FATF encourages Indonesia to address its remaining deficiencies in compliance with FATF standards by fully implementing UNSCR 1267 and improving the legal framework and procedures for freezing terrorist assets.

Myanmar

Myanmar has taken steps towards improving its AML/CFT regime. However, despite Myanmar's high-level political commitment to work with the FATF and APG to address its strategic AML/CFT deficiencies, Myanmar has not made sufficient progress in implementing its action plan, and certain strategic AML/CFT deficiencies remain. Myanmar should continue to work on implementing its action plan to address these deficiencies, including by: (1) adequately criminalising terrorist financing; (2) establishing and implementing adequate procedures to identify and freeze terrorist assets; (3) further strengthening the extradition framework in relation to terrorist financing; (4) ensuring a fully operational and effectively functioning financial intelligence unit; (5) enhancing financial transparency; and (6) strengthening customer due diligence measures. The FATF encourages Myanmar to address the remaining deficiencies and continue the process of implementing its action plan.

More on:

- [Improving Global AML/CFT Compliance: on-going process – 24 October 2014](#)
- [Outcomes of the October 2014 Plenary meeting](#)

Also available

[Déclaration publique du GAFI – 24 octobre 2014](#)

[High-risk and other monitored jurisdictions](#)

Reports

[Mutual Evaluation Reports](#)

[Typologies Reports](#)

[Guidance and Best Practice Reports](#)

[Risk-Based Approach Reports](#)

[Information for the Private Sector](#)

[FATF Business Bulletin](#)

[FATF 30 Years \(1989-2019\)](#)



About

[Who we are](#)

[What we do](#)

[Members and Observers](#)

[FATF Presidency](#)

[FATF Secretariat](#)

[History of the FATF](#)

[Outcomes of meetings](#)

Frequently asked questions

[General questions](#)

[Member Countries and Observers](#)

[Money Laundering](#)

[Mutual Evaluations](#)

[Fraud Warning](#)

More

[FATF Glossary](#)

[Calendar of events](#)

[Job opportunities](#)

[Restricted access for FATF Delegates only](#)

Follow us:

[E-mail Alert](#)

© fatf-gafi 2019. All rights reserved

[terms & conditions](#) | [site map](#) | [contact us](#)

EXHIBIT 22-3



FATF GUIDANCE

National Money Laundering and Terrorist Financing Risk Assessment

February 2013





FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

© 2013 FATF/OECD. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photocredits coverphoto: ©Thinkstock

Table of Contents

ACRONYMS.....	3
1. INTRODUCTION & TERMINOLOGY	4
1.1 Purpose, scope and status of this guidance.....	4
1.2 Core FATF obligations and decisions regarding ML/TF risk assessments.....	5
1.3 Key concepts and terms relevant to ML/TF risk assessment.....	6
1.4 Users of ML/TF risk assessments.....	8
2. GENERAL PRINCIPLES FOR NATIONAL ML/TF RISK ASSESSMENTS.....	9
2.1 Clear agreement on purpose	9
2.2 Determining scope.....	10
2.3 Need for high-level commitment to the ML/TF risk assessment process.....	12
3. ORGANISATION AND INFORMATION	13
3.1 Planning and organisation of the ML/TF risk assessment.....	13
3.2 Sources of information.....	13
3.3 Other planning considerations	18
4. STAGES OF ML/TF RISK ASSESSMENT.....	21
4.1 First stage: identification	22
4.2 Second stage: analysis.....	24
4.3 Third stage: evaluation	27
5. OUTCOME OF RISK ASSESSMENTS	29
ANNEX I. ML/TF RISK FACTORS RELATING TO THREAT	31
ANNEX II. ML/TF RISK FACTORS RELATED TO VULNERABILITIES	39
ANNEX III. EXAMPLES OF NATIONAL-LEVEL ASSESSMENTS.....	50
Australia.....	50
The Netherlands.....	54
Switzerland: Example of a risk assessment used as the basis for applying low-risk exemptions....	55
United States.....	56
ANNEX IV. SPECIFIC RISK ASSESSMENT METHODOLOGIES	57
BIBLIOGRAPHY.....	58

ACRONYMS

AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism
DNFBPs	Designated Non-Financial Businesses and Professions
FATF	Financial Action Task Force
FIU	Financial Intelligence Units
INR. X	Interpretive Note to Recommendation X
ML	Money Laundering
NPO	Non-Profit Organisation
RBA	Risk-Based Approach
SRB	Self-Regulating Body
STR	Suspicious Transaction Report
TF	Terrorist Financing

1. INTRODUCTION & TERMINOLOGY

1.1 Purpose, scope and status of this guidance

1. Identifying, assessing, and understanding ML/TF risks is an essential part of the implementation and development of a national anti-money laundering / countering the financing of terrorism (AML/CFT) regime, which includes laws, regulations, enforcement and other measures to mitigate ML/TF risks. It assists in the prioritisation and efficient allocation of resources by authorities. The results of a national risk assessment, whatever its scope, can also provide useful information to financial institutions and designated non-financial businesses and professions (DNFBPs) to support the conduct of their own risk assessments. Once ML/TF risks are properly understood, country authorities may apply AML/CFT measures in a way that ensures they are commensurate with those risks – *i.e.*, the risk-based approach (RBA) – which is central to the FATF standards as is set out in Recommendation 1, its interpretive note (INR 1), as well as in other Recommendations (*e.g.*, Recommendations 10, 26 and 28).

2. This document is intended to provide guidance on the conduct of risk assessment at the country or national level, and it relates especially to key requirements set out in Recommendation 1 and paragraphs 3-6 of INR 1. In particular, it outlines general principles that may serve as a useful framework in assessing ML/TF risks at the national level. The guidance contained in this document takes into consideration previous FATF work¹, which is still valid reference material. The general principles contained in this paper are also relevant when conducting risk assessments of a more focussed scope, such as in assessments of a particular financial or DNFBP sector (for example, the securities sector) or of thematic issues (for example, the proceeds of corruption related ML). All of these types of assessments (comprehensive, sectoral or thematic) carried out at the national level may also form the basis for determining whether to apply enhanced or specific measures, simplified measures, or exemptions from AML/CFT requirements. Furthermore, while FATF Recommendation 1 does not create specific risk assessment obligations regarding the financing of proliferation of weapons of mass destruction, the general principles laid out in this guidance could also be used in conducting a risk assessment for this area.

3. The guidance in this document is not intended to explain how supervisors should assess risks in the context of risk-based supervision, although risk-based supervision will likely be informed by a national-level risk assessment. Also, this guidance does not provide further explanation of RBA obligations and decisions for financial institutions and DNFBPs. The FATF has issued separate

¹ See bibliography for a list of relevant FATF work, national-level assessments available online and other relevant material. Annex III contains summaries of selected country-level assessment processes.

guidance on implementing the RBA for specific sectors and professions², and that material will be reviewed and, as necessary, modified in light of the revised FATF Recommendations.

This guidance document is not a standard and is therefore not intended to designate specific actions necessary to meet obligations under Recommendation 1 and INR 1 or any other Recommendations dealing with the RBA. Criteria for technical compliance and for assessing effectiveness relevant to this and all other FATF Recommendations may be found in the FATF assessment methodology. The practices described in this guidance are intended to serve as examples that may facilitate implementation of these obligations in a manner compatible with the FATF standards.

4. This guidance is structured as follows:

- This section (1) lays out the purpose, scope and status of this guidance, along with an outline of the core FATF obligations relevant to ML/TF risk assessments at any level.
- Section 2 lays out general principles that should be taken into account when conducting ML/TF risk assessments at the country or national level.
- Section 3 discusses how to organise a national-level ML/TF risk assessment, its frequency, and the data and information that could be used while undertaking such an assessment.
- Section 4 presents a high-level view of the three main stages involved in the ML/TF risk assessment process (identification, analysis and evaluation).
- Section 5 considers the outcome and dissemination of the risk assessment product.
- Annexes to this document contain additional information relating to ML/TF risk assessment including summaries of selected national-level assessments.

1.2 Core FATF obligations and decisions regarding ML/TF risk assessments

5. It is important that the users of this guidance have an understanding of the obligations contained in Recommendation 1 and its interpretive note. This section provides a general outline of these obligations. For more details, reference should be made to the texts of Recommendation 1 and its interpretive note, as well as the FATF assessment methodology.³

6. **Recommendation 1:** The text of Recommendation 1 lays out a number of basic principles with regard to risk assessment. First, it calls on countries to “identify, assess and understand” the ML/TF risks they face, and states that countries should also designate “an authority or mechanism to co-ordinate actions to assess risks”. The goal of the standard is to ensure that countries can

² Nine sectoral RBA guidance papers are available from the FATF website: www.fatf-gafi.org/. This guidance will be revised following adoption of the revised FATF Recommendations in February 2012.

³ See FATF website (www.fatf-gafi.org) for these texts.

mitigate their ML/TF risks effectively, and the risk assessment is clearly intended to serve as the basis for application of the risk-based approach, *i.e.*, “to ensure that measures ... are commensurate with the risks identified.” The text of the Recommendation adds that the “[risk-based] approach” (and therefore the risk assessment process on which it is based) should also be “an essential foundation” in allocating AML/CFT resources efficiently. Furthermore, the Recommendation indicates that risk assessments carried out by countries should be used for determining higher and lower risks that may then be addressed by applying enhanced measures or allowing simplified measures respectively. The Recommendation concludes by requiring that financial institutions and DNFBPs should also be able to identify, assess and take effective action to mitigate ML/TF risks.

7. **Interpretive Note to Recommendation 1:** INR 1 provides more details on the requirement for countries to assess their ML/TF risks and on the purposes for which such assessments may be used⁴. In particular, it emphasises that the objective of the risk-based approach is to ensure AML/CFT measures are commensurate with the “risks identified”, as well as to enable decision making on effective resource allocation. In elaborating on the specific obligations and decisions for countries, INR 1 states that countries should take steps to identify and assess their ML/TF risks on an “ongoing basis.” The objectives of the process at the country level are: (1) to provide input for potential improvements to the AML/CFT regime, including through the formulation or calibration of national AML/CFT policies, (2) to help in prioritising and allocating AML/CFT resources by competent authorities, including through feeding into any risk assessments conducted by such competent authorities (*e.g.*, supervisors) and (3) to feed into the AML/CFT risk assessments carried out by financial institutions and DNFBPs. The text of the interpretive note indicates that supervisors, in accordance with Recommendations 26 and 28, should review the risk assessments prepared by financial institutions and DNFBPs and take the result of that review into consideration in their supervision. The text of INR. 1 also adds that country-level risk assessments should be kept up-to-date, and appropriate information should be shared with all relevant competent authorities, self-regulatory bodies, financial institutions and DNFBPs.

8. In the cases of higher and lower risk determination, country-level risk assessments have very specific roles: Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these risks. Where countries identify lower risks they may decide to allow simplified measures to be applied in relation to some of the FATF Recommendations.

1.3 Key concepts and terms relevant to ML/TF risk assessment

9. In discussing ML/TF risk assessment, it is useful to have a common understanding of certain key concepts and terms that will be used in this guidance. Many of these come from the area of *risk management*, a process commonly used in the public as well as the private sectors to help in decision-making. While many risk management concepts are usefully described elsewhere⁵, their

⁴ Footnote 1 of INR. 1 specifically acknowledges that supra-national risk assessments should be taken into account, where appropriate. It should be noted therefore that the general principles set out in this document that apply to risk assessments carried out by countries at a national level may also be appropriate to risk assessments carried out at a supra-national level. See Section 2 for further discussion of this issue.

⁵ See for example (2009a), ISO (2009b) and ISO (2009c) [see bibliography].

use in this guidance has been adapted to the particular case of assessing ML/TF risk at the national level. Broadly speaking, however, risk management involves developing the appropriate measures to mitigate or reduce an assessed level of risk to a lower or acceptable level.

10. For the purposes of assessing ML/TF risk at the national level, this guidance uses the following key concepts:

- **Risk** can be seen as a function of three factors: *threat*, *vulnerability* and *consequence*. An ML/TF risk assessment is a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand ML/TF risks and serves as a first step in addressing them. Ideally, a risk assessment, involves making judgments about threats, vulnerabilities and consequences, which are discussed below.
- A **threat** is a person or group of people, object or activity with the potential to cause harm to, for example, the state, society, the economy, etc. In the ML/TF context this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present and future ML or TF activities. *Threat* is described above as one of the factors related to risk, and typically it serves as an essential starting point in developing an understanding of ML/TF risk. For this reason, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment. In some instances, certain types of threat assessments might serve as a precursor for a ML/TF risk assessment.⁶
- The concept of **vulnerabilities** as used in risk assessment comprises those things that can be exploited by the threat or that may support or facilitate its activities. In the ML/TF risk assessment context, looking at *vulnerabilities* as distinct from *threat* means focussing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purposes.
- **Consequence** refers to the impact or harm that ML or TF may cause and includes the effect of the underlying criminal and terrorist activity on financial systems and institutions, as well as the economy and society more generally. The consequences of ML or TF may be short or long term in nature and also relate to populations, specific communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector. As stated above, ideally a risk assessment involves making judgments about threats, vulnerabilities

⁶ The United Nations Office on Drugs and Crime (UNODC) has published *Guidance on the preparation and use of serious and organised crime threat assessments* ("The SOCTA Handbook"), which provides useful information on the conduct of national threat assessments related to serious and organised crime.

and consequences. Given the challenges in determining or estimating the consequences of ML and TF it is accepted that incorporating consequence into risk assessments may not involve particularly sophisticated approaches, and that countries may instead opt to focus primarily on achieving a comprehensive understanding of their threats and vulnerabilities. The key is that the risk assessment adopts an approach that attempts to distinguish the extent of different risks to assist with prioritising mitigation efforts.

1.4 Users of ML/TF risk assessments

11. The form, scope and nature of ML/TF risk assessments should ultimately meet the needs of its users – whether these are policy makers, supervisors, operational agencies, financial institutions, DNFBPs, etc. The number and diversity of users of an assessment varies according to the purpose for which it is carried out; however, typical users of risk assessments might include:

- Policy makers and other authorities, for example, in order to formulate the national AML/CFT policies, make reasonable decisions on the legal and regulatory framework and the allocation of resources to competent authorities on the basis of FATF Recommendation 2.
- Operational agencies, including law enforcement, other investigative authorities, financial intelligence units (FIUs), relevant border agencies, etc.
- Regulators, supervisors and self-regulatory bodies (SRBs).
- Financial institutions, and designated non-financial businesses and professions (DNFBPs), for which the national-level ML/TF risk assessment is a critical source⁷ contributing to their own ML/TF risk assessments and risk-based obligations.
- Non-profit organisations (NPOs).
- AML/CFT assessors and assessment bodies more broadly, along with other international stakeholders.
- The general public, as well as academia, specified individuals, etc.

⁷ According to the FATF standard, countries are expected to make appropriate information on the results of their national risk assessment available to financial institutions and DNFBPs for this purpose.

2. GENERAL PRINCIPLES FOR NATIONAL ML/TF RISK ASSESSMENTS

12. The general principles set out below could be considered when a country intends to conduct any kind of ML/TF risk assessment. These include considerations on the purpose and scope of the assessment as well as the process through which an assessment will be conducted; the stages of a risk assessment, the participants, users and other parties involved; the information which may be used, and the final outcome of the assessment process.

13. The nature, methodology, participants, and information required for an assessment depend on the purpose and scope of the assessment. There is no single or universal methodology for conducting an ML/TF risk assessment. Therefore, this guidance does not advocate the use of any particular methodology or process. This guidance is aimed to provide a generic description of the risk assessment process as it might be applied to looking at risk associated with ML/TF and considerations and practical tools for countries to take into account when undertaking their own ML/TF risk assessment.⁸

2.1 Clear agreement on purpose

14. Before starting any kind of ML/TF risk assessment, all parties involved, including those who will conduct the assessment and, as appropriate, the eventual end users should be in agreement on the purpose and scope of the assessment. Expectations should also be set as to how the results relate to the understanding of national-level risks. Generally, a ML/TF risk assessments is intended to help a country to identify, assess and ultimately understand the ML/TF risks it faces. A country may set out more concrete goals for a particular risk assessment however, such as informing the development of policy or the deployment of resources by supervisors, law enforcement and other competent authorities. Understanding the scale and impact of identified risks can also assist in determining the appropriate level and nature of AML/CFT controls applied to a particular product or sector. Given the diversity of potential users and possible diverging expectations, it is essential at the outset that there be clarity about why an assessment is to be conducted, the questions it should answer, the criteria that will be used to answer those questions and the possible decisions that the assessment will feed into.

15. ML/TF risk assessments may be tied to strategic planning and linked to specific actions or decisions. For example, a national ML/TF risk assessment serves as input to a national AML/CFT strategy or policy as part of the country's domestic AML/CFT co-ordination process. The purposes of the assessment will also vary according to the needs of the users. The purpose and scope of the assessment may also determine the methodology that is to be used.

⁸ Nonetheless, those involved carrying out a national ML/TF risk assessment may gain further insight into risk concepts, methodologies, processes, and tools from consulting any requirements of their own government relating to risk assessment or other material on risk management standards and associated publications (see the bibliography at the end of this document for a list of some of these sources).

2.2 Determining scope

Money laundering and terrorist financing

16. A key consideration when deciding on the scope of an ML/TF risk assessment is to determine whether ML and TF risks should be assessed separately or together. Factors associated with TF that might need to be considered may be very different from those associated with ML. For example, funds used for financing of terrorist activities may be derived from criminal activity or legal sources. In addition, a key focus in combating TF is on preventing future terrorist acts from occurring whereas with combating ML, the criminal activity (the predicate offence) has already taken place. Another difference is that, transactions associated with TF may be conducted in very small amounts, which when not viewed in the TF context could be the very transactions that are frequently considered to involve minimal ML risk. Countries may therefore choose to assess their ML and TF risks separately.⁹

National, supranational and sub-national risk assessments

17. As stated throughout this guidance, ML/TF risk assessments may be undertaken at different levels and with differing purposes and scope, including supranational assessments (of a group of countries), national (or country level) assessments and sub-national assessments (of a particular sector, region, or operational function within a country) even though the basic obligation of assessing and understanding ML/TF risk rests on the country itself. In order to be of use in assessing and understanding national-level risks, it is helpful that assessments carried out at other levels relate to each other in a consistent way, although it is recognised that this may not be possible in all instances due to specific risks and the specific assessment approach undertaken. For example, the interplay between a national ML/TF assessment and specific sectoral ML/TF risk assessments could be considered as follows:

- High or low risk situations identified by the competent authorities through national ML/TF assessment should logically influence and/or confirm choices of higher, lower, or low risk situations relevant to the risk-based approach as implemented by financial institutions and DNFBPs, and overseen by supervisors or SRBs.
- Continuing examination by financial institutions and DNFBPs of their risks (regarding types of customers, products, etc.) as monitored by supervisory agencies would potentially contribute to and/or confirm identification of risk levels in the context of national ML/TF assessments.

18. In principle, a national ML/TF risk assessment can be composed of different types of assessments, and the different levels could be combined together to form a national-level understanding of the risk with each limited-scope assessment contributing to the overall picture. It may, for example, be possible for those conducting the ML/TF assessment to rely on a variety of assessments (for example, assessments conducted by supervisors and SRBs on the ML/TF risks in

⁹ For the purposes of ML/TF risk assessment, this guidance discusses indicators or elements relating to ML and TF in Section 4 under the explanations of identification and analysis. Further relevant lists are provided in Annexes I and II.

financial and DNFBPs sectors, ML/TF risk assessments conducted by the firms operating in the financial and DNFBP sectors, threat assessments conducted by law enforcement agencies and FIUs on ML¹⁰ and TF, assessments of the ML/TF vulnerabilities in the NPO sectors or legal persons and arrangements, and any ML/TF assessments carried out at the state level in a federation) to form a national-level understanding of the ML/TF risk.

19. The approach adopted by each country may also be dependent on the country's framework for co-ordinating and co-operating on AML/CFT matters. For example, in some cases, it might be more appropriate to pull together all or many of the relevant contributors to conduct a single national ML/TF risk assessment. This would also simplify the need to collate and compare different types of assessments and allow for more direct exchange of information between the contributors. In other cases, where the ML/TF risks are diverse and differ between regions, or where the competent authorities have to deal with very specific risks or need to conduct an assessment to justify exemptions on the basis of low ML/TF risks, it may be more appropriate to have targeted, sectoral or thematic risk assessments which the national authorities would then use in developing a national-level understanding of the ML/TF risks.

20. The size and complexity of the country, its ML/TF environment, and the maturity and sophistication of the AML/CFT regime may also influence how a country decides to assess and understand its ML/TF risks. Ideally, a national-level ML/TF assessment should attempt to focus on macro-level risks affecting the AML/CFT regime. For example, it may focus on the potential abuse of sectors rather than of individual institutions, or the adequacy of resources across a linked group of AML/CFT competent authorities rather than individual authorities, and so on. The degree of aggregation or disaggregation of risks to focus on will be country specific.

Comprehensiveness of assessment

21. Regardless of the approach adopted, countries are advised to ensure that their assessment of ML/TF risk is comprehensive enough to provide an overall picture of the national ML/TF risks across the AML/CFT regime. Ideally, this picture should include sufficient breadth and depth about potential threats and vulnerabilities and their consequences to address the purpose and scope of the assessment. The range of threats and vulnerabilities relevant for any particular assessment will thus vary according to the scope of the assessment (national, regional, sectoral, etc.); however, the country will need to ensure that all relevant risks are taken into account when the results from different types of assessments are combined to derive national-level ML/TF risks. Where information gaps exist or difficulties in reaching conclusions arise, it is useful if these can be recognised in the risk assessment and then become areas where more work is required in the future. In addition, the uncertainty caused by the lack of information may itself raise the risk profile of the issue under consideration. In seeking to develop a comprehensive picture, those in charge of the ML/TF risk assessment need to identify and acknowledge these limitations as they make a determination of the risks that can be assessed. Future risk assessments may be able to seek new or alternative sources of information that will permit assessment of areas that could not be adequately or fully assessed in an earlier work.

¹⁰ Again, UNODC (2010) mentioned above may be relevant in this regard.

2.3 Need for high-level commitment to the ML/TF risk assessment process

22. Before conducting an ML/TF risk assessment, it is essential that there be the political will to carry out this work and ensure that the objectives of the assessment can be achieved. This political will may be demonstrated in a clear commitment from high-level government officials to the ML/TF risk assessment exercise. These officials will need to recognise, understand and acknowledge any ML/TF risks that exist within their country and how these risks may be distinct from larger criminal or terrorism related threats. Situations where government officials (or competent authorities) purposely fail to identify ML/TF risks in their country (or they deliberately determine certain risks as low level) because they believe that acknowledgement of a higher risk level may damage their reputation or may have a negative effect on investment within the country and its financial sector need to be avoided.¹¹ Appropriate judgment and balance are therefore important in the conduct of the national ML/TF risk assessment process to prevent the process from becoming unduly influenced by or subordinate to a particular policy approach, legislative reform, agency agenda, resource injection, or lobbying by a specific stakeholder.

¹¹ Examples of situations where ML/TF risks are often not acknowledged include those where a country itself may have little criminal or terrorist activity but its vulnerabilities attract foreign funds for laundering or financing activity or its residents send funds abroad to support foreign terrorists and terrorist groups.

3. ORGANISATION AND INFORMATION

3.1 Planning and organisation of the ML/TF risk assessment

23. In establishing a ML/TF risk assessment process, some countries may choose to establish a more formal inter-agency working group or the like to oversee their risk assessment process. Round-table discussions, working groups of experts and taskforces of relevant agencies and bodies are other examples of how such a process may be organised. It is useful if the process is as inclusive and co-operative as possible. However, ideally there should be a clear determination and designation of the specific agency, organisation or “task force” in charge of leading and co-ordinating the process. See Annex III which contains examples of national-level assessments for specific ways that countries have organised their assessments.

24. As mentioned in the previous section, the purpose and scope of the particular assessment will likely determine the composition of the risk assessment “team”. Meetings, interviews, data gathering, and analysis related to national-level ML/TF risks can be a lengthy process, particularly if there is disagreement among competent authorities on the threats and vulnerabilities. A clear project plan describing the process, roles and responsibilities of various partners for identifying, assessing and understanding the country’s ML/TF risks may therefore be useful. In addition, an appraisal of likely resource requirements needed to undertake the ML/TF risk assessment may be beneficial.

25. There are a variety of processes through which a country may reach an informed understanding of the risks it faces – in a particular situation or overall. This includes top-down approaches (resulting from a single, co-ordinated framework or system) and bottom-up (building a national assessment from a patchwork of assessments with a smaller scope). It also includes organic processes which may develop an understanding of risk incrementally, for example by starting with a limited or specific focus assessment and gradually expanding it whilst learning from the experience of the preceding work.

3.2 Sources of information

Contributors to the risk assessments

26. While some aspects of the ML/TF risk assessment may be conducted through a single agency process, in most cases, it is unlikely that one organisation by itself possesses all necessary information and data to adequately perform such a task at the national-level. It is therefore advisable that a national-level ML/TF assessment exercise involve a broad range of relevant departments, agencies and other organisations within the government (federal and other levels as applicable) that have AML/CFT responsibilities, expertise or both. This includes those with knowledge of the types and scope of proceeds-generating offences, those that can identify AML/CFT regime vulnerabilities and those with other critical related information. Contributors that may provide essential input to the national-level ML/TF risk assessment process include the following (see also Figure 1):

- *Policy-making bodies*: Policy making bodies should, where relevant, be included in the conduct of a risk assessment – not necessarily as providers of information, but as the principal users of risk assessments – in order to ensure that risk assessments adequately address high-level questions and that any implications of the risk assessment for the revision of national AML/CFT policies are identified. They have a particular role to play in helping frame the scope of the risk assessment exercise.
- *Law enforcement and prosecutorial authorities* (including police, customs/border control, and criminal intelligence agencies where appropriate): These operational authorities may be able to provide information on specific cases involving the particular area under assessment and may also assist, where possible, in estimating amounts of proceeds of crime based on information on predicate offence. They thus are likely to play a central role as a source of information for the process. They may also have relevant statistics on ML/TF investigations, prosecutions and convictions, assets seized / confiscated / repatriated / shared and other (international) co-operation requests or hold information about criminals' *modus operandi* obtained during the course of an investigation. They may also be able to provide information on new trends and risks detected through their investigations as well as assist in identifying vulnerabilities.¹²
- *Intelligence and/or security services*: These agencies may be particularly relevant to assessments of terrorism and terrorist financing, where much of the available information on threats may come from intelligence sources¹³. Such agencies may also function as centres of expertise on intelligence analysis, and can provide external review or validation of risk or threat assessments using intelligence analysis and assessment methodologies, where these are available. They may also be able to assist in identifying vulnerabilities.
- *Financial intelligence units*: On the basis of the suspicious transaction reports (STRs) and other information it receives and the strategic analysis it conducts, the FIU is ideally placed to identify threats, vulnerabilities, ML/TF techniques, methods and trends, including new patterns¹⁴. FIUs may be able to extract from their databases information on specific products or transaction types that can be either converted into sanitised cases and/or

¹² Some of this information may be available from other authorities such as Justice Ministries and other agencies.

¹³ However, this may involve information of a sensitive nature which could limit the exchange by intelligence or security services.

¹⁴ See INR 29 which describes the role of the FIU in conducting strategic analysis and its role in helping establish policies and goals for other agencies within the AML/CFT regime. At the same time, it may be advisable not to rely too heavily or solely on FIU statistics as these often derive from suspicion about potential ML or TF activity rather than actual cases.

aggregated to reveal a trend. This information can be supplemented by statistics on the reporting of transactions by the reporting entities.

- *Regulatory and supervisory authorities* (including, for example, self-regulatory bodies and any FIUs with such responsibilities) often have the benefit of having a good picture of the institutions regulated for AML/CFT within their countries. Through their AML/CFT inspection and monitoring, either on-site or off-site, they gain a unique knowledge of specific vulnerabilities associated with types of institutions, products, transactions (including those of a cross-border nature) and customers that can be associated with ML/TF and are able to assess a sector's policies, procedures and controls. They are therefore in a position to provide views on whether a particular risk is being adequately identified and managed.
- *Other authorities* such as Foreign Ministries (for example, threats identified by the UN) or statistics agencies may also hold information that can inform the risk assessment exercise and could participate directly or indirectly. Likewise, agencies that may have information about particular criminal activities or predicate crime may also be able to contribute (for example, welfare ministries in relation to welfare fraud, tax authorities in relation to tax crimes, anti-corruption agencies in relation to corruption etc.).
- *International and foreign partners*: FATF-style regional bodies (FSRBs) of which a country is a member may also be a useful source of information on risk, in particular regarding work carried out elsewhere in the region to identify and understand risk. Similarly, foreign partners, such as authorities from other countries, may also be a potential source of information.

Involvement of the private sector and other actors

27. Private sector involvement may also be valuable in building a complete picture of national ML/TF risks and may benefit the assessment process in a number of ways – as either as a source of information or by having representatives participating directly in some aspects of the process if the country considers that appropriate. It is also important to consider that sometimes the private sector may have commercial interests that might preclude a completely impartial view of ML/TF risk. Therefore, while the private sector may not in all countries be an active participant in the national ML/TF assessment, it may be the best source of information in many areas. Contributors from the private sector that may provide essential input to the national-level ML/TF risk assessment process include the following:

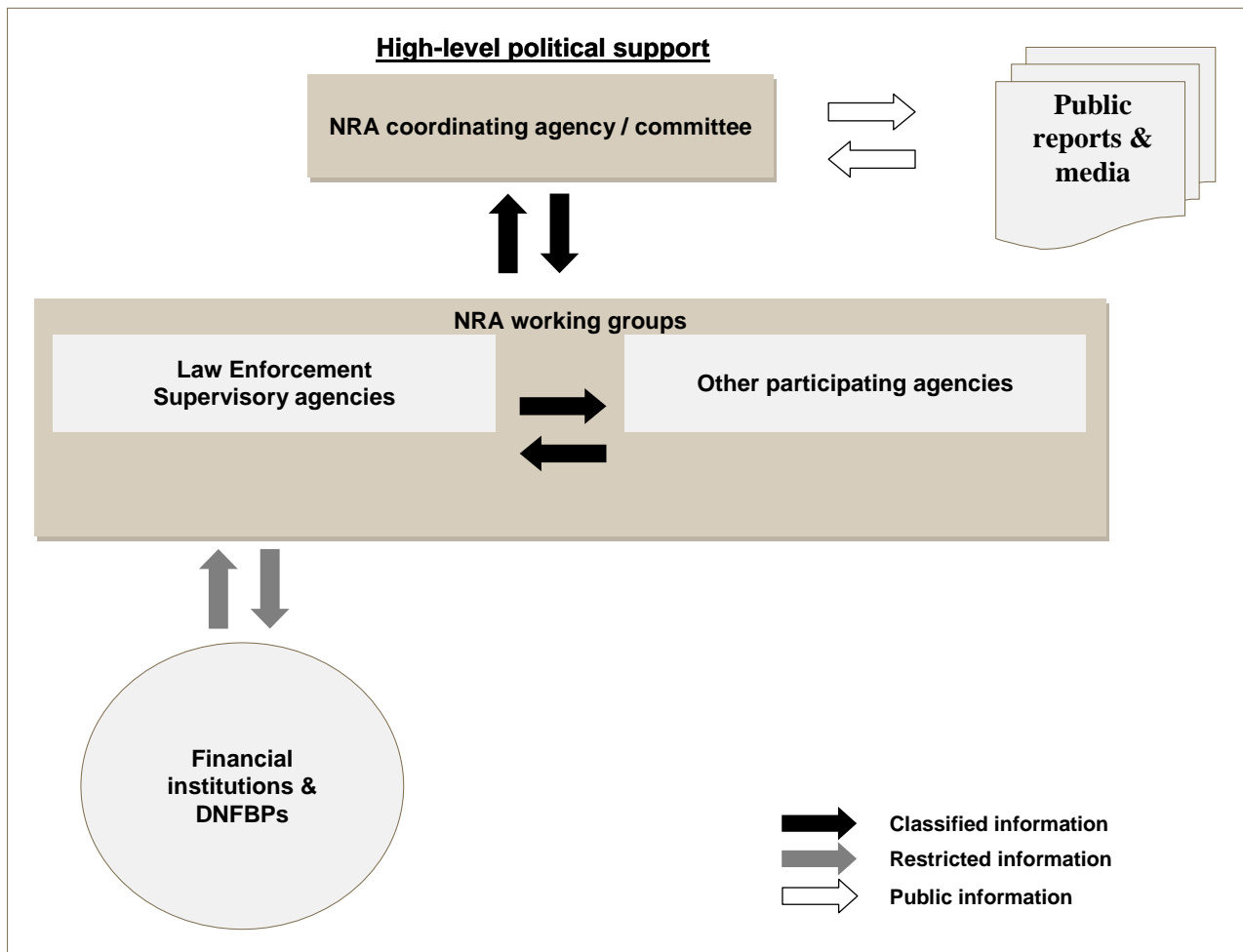
- *Financial institutions and DNFBPs*: When applying the risk based approach to implementing AML/CFT preventive measures, financial institutions and DNFBPs may have already conducted ML/TF risk assessments of their own, and such assessments could also be an important contribution to national-level assessments. More generally, financial institutions and DNFBPs and their staff or representatives may have valuable information on the structure, organisation and size of sectors, their customers as well as the

features and characteristics of particular financial products to help with determining the level of risk presented and to assist in identifying vulnerabilities. As stated in the introduction, the private sector is also a potential key user of any ML/TF risk assessments conducted at national level. It should be noted as well that Recommendation 1 now requires countries to have mechanisms to provide appropriate information on the results of national ML/TF risk assessments to financial institutions and DNFBPs.

- *Industry associations and self-regulatory bodies (SRBs)* with a broad and representative membership in the area of the assessment may provide essential aggregated statistics, such as particular types of transaction volumes and industry-wide information.
- *Other actors:* researchers, criminologists, industry associations, private sector experts (for example, practitioners or others with in-depth knowledge of specialised financial activities), risk management experts, non-government organisations and civil society, academics and other international experts/specialists can provide their perspectives, for example, on what constitutes a “cash intensive” business or economy, produce reports and provide analysis related to ML/TF and predicate crimes. It may be very useful to develop risk assessment methods and the monitoring of the risk assessments by actors with expertise in scientific research.
- *Criminals* could also be a valuable source of information, particularly in jurisdictions where they are given the incentive to “repent” or share information in return for favourable treatment in the criminal justice system. They can explain the reasons why one sector or product or transaction or (more broadly) *modus operandi* was chosen rather than another. While it may be difficult to obtain such information from them directly, there may be indirect methods such as obtaining copies of research into their behaviour or working with prison or custodial authorities to obtain valuable information that they may hold. Court reports, sentencing and transcript records can also be a rich source of information on the motives and methods used by money launderers and terrorist financiers.

28. As a targeted ML/TF risk assessment may focus on a specific sector, only a small number of private sector representatives (for example, from an industry association or SRB) might be involved. A comprehensive national risk assessment on the other hand is of a larger scope and could attract more participation from a wider segment of the private sector. Time and resources to co-ordinate input and obtain agreement among participating bodies need to be considered when planning to undertake large-scale ML/TF assessments that involve extensive consultation.

Figure 1. Interrelationships between various contributors to the risk assessment process



Information and tools required for ML/TF risk assessments

29. The quality of the risk assessment exercise depends largely on the types and quality of data and information available. While quantitative assessments (*i.e.*, based mostly on statistics) may seem much more reliable and able to be replicated over time, the lack of available quantitative data in the ML/TF field makes it difficult to rely exclusively on such information. Moreover, information on all relevant factors may not be expressed or explained in numerical or quantitative form, and there is a danger that risk assessments relying heavily on available quantitative information may be biased towards risks that are easier to measure and discount those for which quantitative information is not readily available.

30. For these reasons, it is advisable to complement an ML/TF risk assessment with relevant qualitative information such as, as appropriate, intelligence information, expert judgments, private sector input, case studies, thematic assessments, typologies studies and other (regional or supranational) risk assessments in addition to any available quantitative data. Similarly, objective data can be complemented by surveys or information of subjective nature such as perception indexes. Countries may in the long term wish to consider harmonising and further developing their quantitative data collection mechanisms that are used for ML/TF risk assessment in line with the FATF Standards (for example, Recommendation 33) and international best practices. It is essential

that all participating organisations be authorised to share potentially sensitive information. Such information should be received, exchanged and used in accordance with agreed procedures, policies and applicable laws and regulations.

31. Determining the sources of data, type of information, tools, and which analytical techniques will be used is therefore essential in conducting ML/TF risk assessments. In order for a national ML/TF risk assessment to arrive at the most accurate findings, it is advisable that as much analysis and conclusions within the assessment as possible be based on objective information. The information used in a ML/TF risk assessment may be derived from various sources (both qualitative and quantitative). The availability and quality of information will vary considerably by country. Countries, including low capacity countries, with limited data on criminal investigations or financial transactions will still be able to conduct a risk assessment but may need to rely more on expert judgment and international sources of data after they have obtained all available data from national sources. More generally, some officials may find it beneficial to engage independent experts with substantial experience in risk assessment to carry out some aspects of the risk assessment rather than try to carry out the whole process themselves.

32. A national ML/TF risk assessment may conclude that one of the significant vulnerabilities is the presence of information gaps within the AML/CFT regime that need to be closed. Thus, the risk assessment can also reveal the adequacy of the available data and give directions for potential data and information sources, as well as future data collection requirements. A review of the available data and information within a country's AML/CFT regime as an essential component of the ML/TF risk assessment process also helps identify the extent to which any lack of data and information is a systemic vulnerability in the country.

33. Maintaining a consistent approach to the risk assessment process and using the same quantitative and qualitative indicators where possible is important to enable a comparison of findings over time. However, the desire to compare results between one assessment and the other or after periodic updates should not override the need to improve the methodological process or add new data sources as appropriate. Indeed, the experience obtained from conducting an ML/TF risk assessment – when properly documented – may help a country to refine future assessments or adopt an entirely new and more effective approach in subsequent assessments.

34. When looking at money laundering and terrorism financing trends, a country's international financial transactions may also be a key element. Information on cross-border financial flows is a valuable source of data which needs to be considered. In addition, a number of countries have extensive reporting processes on crimes related to money laundering, such as human trafficking or organised crime and some international organisations collate statistics on these and other relevant crimes. These reports can be an important source of information for assessing national ML/TF risks.

3.3 Other planning considerations

Frequency of the risk assessment

35. Recommendation 1 requires that countries assess risks “on an ongoing basis”, and that they keep assessments up-to-date. The authority or mechanism designated to assess ML/TF risks in the

country will likely be responsible for ensuring that this obligation is met. Recommendation 1, however, does not specify a particular period of time. Therefore, the frequency with which a risk assessment is updated is determined by the country, based on a number of factors, including how quickly (and how significantly) the risks may change.

36. Following the initial assessment of a specific area, the entire process does not necessarily need to be repeated at pre-specified points in time. However, it is advisable that the authority or mechanism designated to assess ML/TF risks proposes after the first national-level ML/TF risk assessment when the next risk assessment should be carried out, for example, within the next three to five years. It should also be emphasised that carrying out an ML/TF risk assessment should be considered as an evolutionary process. As indicated above, the lessons learned from an initial risk assessment may help to inform subsequent updates or future risk assessments, and this may also be a factor in determining the frequency.

37. Some factors that could also influence the need for updating or conducting a new ML/TF risk assessment process include: when new ML or TF activity causes substantial harms to occur, or new intelligence or typologies become available or where significant changes are made to products and services (including their operating environment). A number of developments (domestically and internationally) may also prompt the need to review a risk assessment:

- Changes in international standards or guidance (for example, FATF recommendations, IOSCO, IAIS, guidance and sound practice papers issued by the Basel Committee on Banking Supervision, UN Conventions, EU legislation).
- Changes in the political, economic or legal framework of a country.
- Developments in other countries' regimes (in particular the country's important trading partners or countries with similar financial sectors or legal systems).
- Issues raised by the private sector (for example, "level-playing field", "countries of concern" not already identified by FATF, new products, services and technologies).
- Open source material or public reports (for example, FATF typology reports) on new ML or TF trends.
- Domestic typologies studies and intelligence received from law enforcement, the FIU and other stakeholders, which may include updates on the vulnerability of a product or service.
- Information about trends in other countries (by means of international conferences, regular information exchanges, etc.).
- The cycle of mutual or self-evaluation may also be an important consideration for countries in deciding when to conduct or update their risk assessment.

Documentation of methodologies and processes used

38. Regardless of the method or process used to conduct the ML/TF risk assessment exercise, it is advisable that the designated authority or mechanism responsible for assessing a country's ML/TF risks record sufficient information about the methodologies and processes to be used. This is to ensure that all parties involved in the process are aware of their obligations and responsibilities and to assist with demonstrating to other stakeholders, including assessors, how the risk assessment was conducted. Such an approach is also appropriate for the purposes of transparency and accountability.

39. While not all the information and analysis of the risk assessment may be shared broadly, it is essential that the designated authority in charge of co-ordinating the process ensure that adequate records of the data, information, analysis and conclusions are kept securely. Such records allow for the preservation of institutional memory and in explaining the rationale for past risk-related policy decisions, permit future updates, and ensure the consistency in future risk assessments endeavours. Countries can use this body of information to inform AML/CFT assessors about the adequacy of their risk assessment process, subject to restrictions on sharing sensitive information.

Supra-national risk assessments

40. Assessments conducted at a supra-national-level may be of value in country-level or national risk assessments. Such assessments may serve as an additional source of information in conducting risk assessments at the country level and could, for example, help in the identification of threats, vulnerabilities and their consequences. They may also provide a benchmark for certain judgments made in subsequent risk assessments at the country level. It is also worth noting that supranational assessments can themselves be informed by the results of country-level risk assessments.

Links with global ML/TF assessment

41. The FATF Global Money Laundering and Terrorist Financing Assessment was adopted by the FATF in June 2010. The Global ML/TF Assessment provides an overview of the ML/TF threats as identified by the FATF (and therefore on a worldwide or "global" level) along with the ultimate harms that they can cause. The aims of the Global ML/TF assessment are to inform governments, the private sector and international policy-makers about ML/TF threats in order to better manage scarce resources and to take more focused actions against ML/TF. The issues identified in the assessment may be useful to governments when conducting national ML/TF assessments. The Global ML/TF Assessment may therefore provide an important part of the context for any assessments undertaken at national level.

42. Only a few countries have previously carried out national risk assessments, but it is envisaged that the production of national-level risk assessments will become a more important contributor to the Global ML/TF Assessment effort. Therefore there is a two-way relationship between this assessment and national ML/TF risk assessments with each benefiting from information contained in respective assessments.

4. STAGES OF ML/TF RISK ASSESSMENT

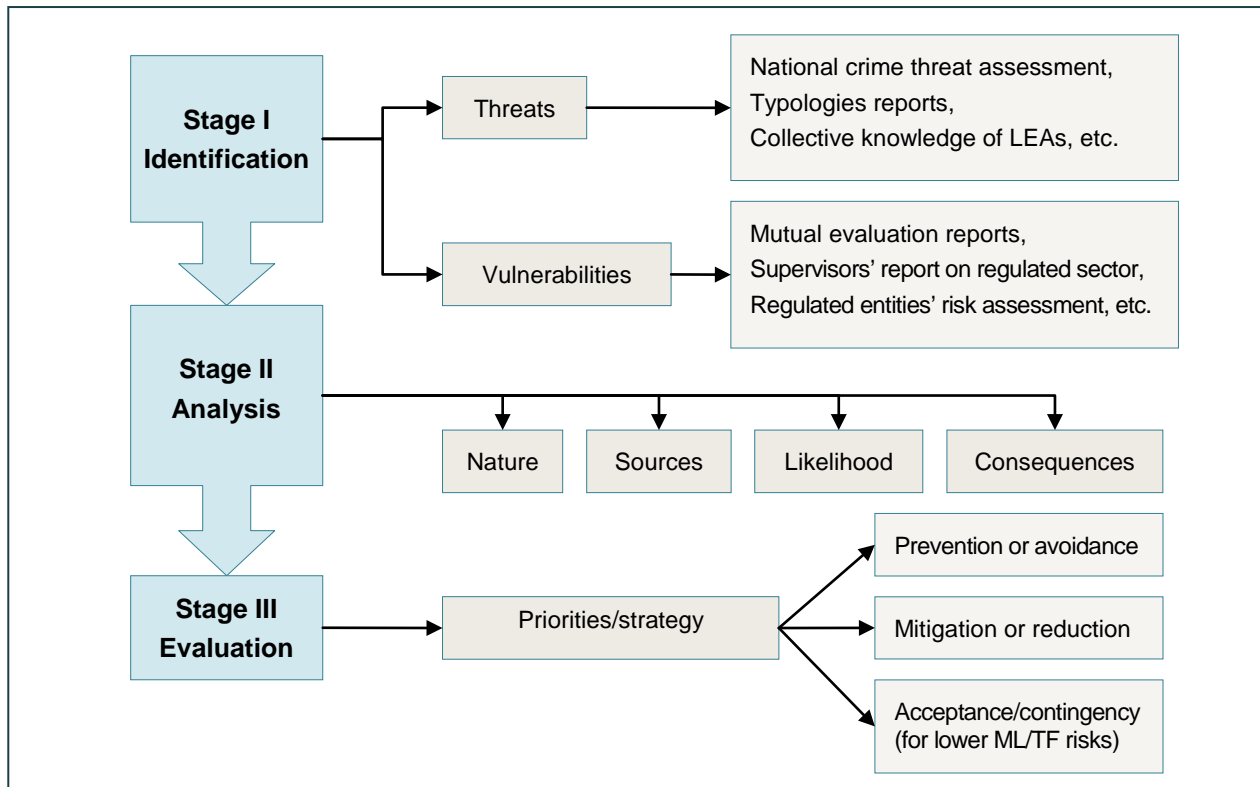
43. The process of risk assessment can be divided into a series of activities or stages: *identification*, *analysis*, and *evaluation*. The three stages are briefly described in this section. For completeness all three stages are described; however, this guidance focuses mainly on the first two. Figure 2 below provides an overview of the ML/TF risk assessment process.

- In general terms, the process of **identification** in the context of an ML/TF risk assessment starts by developing an initial list of potential risks or risk factors¹⁵ countries face when combating ML/TF. These will be drawn from known or suspected threats or vulnerabilities. Ideally at this stage, the identification process should attempt to be comprehensive; however, it should also be dynamic in the sense that new or previously undetected risks identified may also be considered at any stage in the process.
- **Analysis** lies at the heart of the ML/TF risk assessment process. It involves consideration of the nature, sources, likelihood and consequences of the identified risks or risk factors. Ultimately, the aim of this stage is to gain a holistic understanding of each of the risks – as a combination of threat, vulnerability and consequence in order to work toward assigning some sort of relative value or importance to them¹⁶. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk and the purpose of the risk assessment, as well as based on the information, data and resources available.
- **Evaluation** in the context of the ML/TF risk assessment process involves taking the risks analysed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to development of a strategy for their mitigation.

¹⁵ The term *risk factors* is used to refer to specific threats or vulnerabilities that are the causes, sources or drivers of ML or TF risks.

¹⁶ As stated in Section 1 under the descriptions of relevant concepts, a risk assessment at the conceptual level involves gaining a comprehensive understanding of all three components of ML/TF risk (threat, vulnerability *and* consequence). The practical challenges in describing ML/TF consequences in a meaningful way may lead countries to focus first and foremost on identifying ML/TF threats and vulnerabilities. The recognition that there are specific consequences of ML/TF threats and vulnerabilities is nevertheless important, as this component, even if understood at a theoretical level may help in assigning a relative value or importance to various ML/TF risks.

Figure 2. Overview of the ML/TF Risk Assessment Process



4.1 First stage: identification

44. After establishing the purpose and scope for the risk assessment exercise, a first step is to identify risks to be analysed. Given that ML/TF risks – as stated earlier in this guidance – are a combination of threats, vulnerabilities and consequences, a good foundation for the identification process is to begin by compiling a list of the major known or suspected threats and vulnerabilities that exist based on primary methods and payment mechanisms used, the key sectors which have been exploited, and the primary reasons why those carrying out the ML/TF are not apprehended and deprived of their assets. The identified ML/TF threats or vulnerabilities should of course relate to the purpose and scope of the assessment and this will also influence whether they are more micro or macro in focus.¹⁷

45. At this initial stage, the list may be broad or specific, be based on actual or known typologies, or drawn from a more generic list of types of cases or schemes or circumstances involved in the ML or TF processes. For ML/TF threats, the development of a list may be facilitated by having access to, for example, national crime threat assessments¹⁸, typologies reports, as well as the collective

¹⁷ Decisions will need to be made about the level of aggregation or detail with which the list of threats and vulnerabilities is expressed (along with the risks derived from them), and this will be influenced by the size and complexity of the country. A more focussed ML/TF assessment will typically involve a narrower range risks but it may provide more opportunity for those to be expressed using a higher level of detail than for a national level assessment.

¹⁸ Again, the UNODC (2010) mentioned above may be relevant in this regard.

knowledge of law enforcement. Formulating a list of the country's major ML/TF vulnerabilities will typically be informed by the likes of mutual evaluation reports¹⁹ of compliance with the FATF Recommendations²⁰, reports by supervisors and about vulnerabilities in the regulated sector, risk assessments prepared by regulated entities, and the collective knowledge of the authorities involved in AML/CFT, particularly regarding the existence and effectiveness of any general mitigants or controls that help combat ML/TF (such as limits on cash use in certain transactions) and any weaknesses in how they carry out their responsibilities, including because of a lack of resources. The exercise of establishing this first list of threats and vulnerabilities should consider the full process of ML or TF, including the international/cross-border context. Thus, discussion of ML or TF threats will probably need involvement of appropriate experts who contribute to compiling this initial list of the main or common ML/TF threats and vulnerabilities.

46. ML/TF risks exist when ML/TF threats exploit ML/TF related vulnerabilities. Thus after compiling a list of ML/TF threats and vulnerabilities, the next focus is for those involved in the process to think about how these interact and articulate a list of risks the country faces when combating ML/TF.²¹ It should be stressed that something identified on the list at this stage is not automatically classified as having higher (or lower) risk – it has simply been identified as sufficiently relevant to go into mix of risks to be analysed.

47. There are different approaches that may be used at the identification stage. One is based on identifying risk *events*, which involves starting from specific examples of ML or TF events – which may be macro or micro in nature. Under this approach the participants identify the main risk scenarios to analyse. Some examples of specific ML/TF risk events (derived from the threats, vulnerabilities and consequences) identified at this stage might include the following²²:

- “Organised crime groups place proceeds of crime into the financial system through co-mingling cash with legitimate business takings.”
- “Narcotics trafficking groups use cash smuggling to move illegal proceeds over the border.”
- “Terrorist group X is known to raise funds via cash donations obtained within the country.”
- “Foreign terrorist groups uses domestic NPOs as fronts for terrorist financing activities.”

¹⁹ And detailed assessment reports.

²⁰ Any of these reports may contain outdated information due to the length of time since the last assessment. This material may therefore be supplemented by other material developed through subsequent follow-up or monitoring processes.

²¹ Some country ML/TF risk assessment processes may wish to move straight to articulating a list of ML/TF risks without identifying threats and vulnerabilities separately

²² See Annex I for a more lists of examples of predicate offences (threats) for money laundering and see Annex II for a list of vulnerability related factors. These may be of assistance in developing lists of threats, vulnerabilities, and consequences during ML/TF risk assessments. It is important to note however that these lists are not exhaustive.

- “Foreign criminal groups launder foreign proceeds of crime in the country by investing in the domestic real estate sector.”
- “Criminals and terrorists exploit the lack of information on beneficial ownership and control of companies to obscure or hide links between them and legal persons controlled or owned by them.”
- “Terrorists / criminals move funds out of the country via informal money transfer businesses.”
- “Financial institutions fail to identify suspicious transactions because of poor monitoring systems.”
- “Law enforcement fails to investigate ML due to their focus on predicate crime only.”
- “Launderers avoid conviction due to poorly drafted ML laws.”
- “Law enforcement are unable to investigate some ML and TF cases due to poor information about beneficial ownership and control of companies used by launderers and financiers.”
- “Confiscation of proceeds of crime fails because law enforcement fail to use provisional measures to freeze or seize assets during investigations.”

48. Another approach that may be used starts from a macro-level and tends to focus more on circumstances. Under this approach a list of risk factors (relating to threats and vulnerabilities, see Annexes I and II for some examples of risk factors) is identified for analysis. The list can be expanded or narrowed down depending on the scope of the ML/TF assessment.

49. Irrespective of which approach is used for identification, those involved in the process must keep an open mind to ensure that all relevant risks or risk factors are identified so as to avoid inadvertently overlooking key issues that contribute to the country’s ML/TF risk. The actual processes used to identify the initial list of risks will vary. Some countries may utilise more formal techniques such as surveys and quasi-statistical analysis of past events or circumstances while others may carry out a brainstorming exercise among appropriate experts to produce a list or perhaps a tree diagram of related events or circumstances. Once an initial list of risks is identified, the assessment process can proceed to the next stage.

4.2 Second stage: analysis

50. *Analysis* lies at the heart of the ML/TF risk assessment process. It is through analysis that the process moves from a mere description of the ML/TF risks facing a country – akin to a situation report – to fuller understanding of the nature, extent and possible impact of those ML/TF risks. As indicated in the introduction, risk can be thought of as a function of *threat*, *vulnerability* and *consequence*. The goal of this step is therefore to analyse the identified risks in order to understand their nature, sources, likelihood and consequences in order to assign some sort of relative value or importance to each of the risks.

51. Ideally, such analysis takes into account the relevant “environmental” factors -- in the broadest sense -- which influence how the risks evolve. These broad “environmental” factors include the general circumstances of the country (for example, relevant political, economic, geographical and social aspects), as well as other structural or specific contextual factors which could influence the way AML/CFT measures are implemented. Determining which environmental factors are relevant to ML and TF (and thus influence the nature, sources, likelihood and consequences of the identified risks) can be assisted by thinking of them in terms of the political, economic, social, technological, environmental and legislative factors that may enable or facilitate the particular risk. In practical terms, many of these factors will have already been identified as among some of the vulnerabilities facing the country (See Annex II).

52. In practice, not all broad environmental factors will be applicable to every ML/TF risk assessment. Indeed, the individual factors will vary from country to country and may evolve over time. It is important to ensure that factors looked at are indeed relevant, and it may therefore be necessary to use some of the methods (surveys, brainstorming) mentioned above to agree on which factors to consider in a particular ML/TF assessment process. In addition, it may become apparent in thinking about some of these factors that certain ML/TF risks might not have been identified at the first stage. As stated previously, the process – even at the analysis stage – should be flexible enough to make adjustments to modify (add to, delete or combine) the risks identified in stage one of the process.

53. Having considered the influence of the broad environmental factors on each identified risk the analysis stage can move on to attempting to determine the size or seriousness of each risk. Often this may mean determining the size or seriousness of the risk in relative terms to other risks. This can be done by using different techniques, for example:

- If doing this holistically, those involved in the risk analysis might collectively rank or categorise each of the identified risks in terms of their degree and relative importance.
- More formal analytical techniques can involve identifying the nature and extent of the consequences of each risk along with the likelihood that the risk may materialise and combining those results to determine a level of risk, which is often presented through the use of a matrix. The actual processes used to identify consequences and determine likelihood can also vary: Some countries may choose to employ more formal techniques such as surveys of experts or statistical analysis of the frequency of past ML or TF risk related activity. Others may choose to rely on the conclusions of a group discussion or workshop to help develop this information.

Understanding the consequences associated with ML and TF

54. In the process of analysing ML and TF risks, it is crucial to have a general understanding of why ML and TF occur. The acts of laundering money and financing terrorism are done to facilitate crime and terrorism more broadly. Profit is fundamental to the goals of most crime and therefore criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds. In order for terrorists to carry out

their operations, attacks or maintain an infrastructure of organisation support, the need to have the ability to collect, receive and move funds. The availability of working capital is also fundamental for both criminals and terrorists to sustain their networks.

55. It is equally important to understand the consequences associated with the activity described above. This will assist in reaching conclusions about the relative importance of each identified risk. The consequences of this illicit financial activity are often viewed at the national or international level but also affect the regional, local and individual levels. Both *impacts* and *harms* (which make up consequences) can be further categorised into types, such as physical, social, environmental, economic and structural²³. From a national perspective, one of the main consequences of ML and TF is that it has a negative effect on the transparency, good governance and the accountability of public and private institutions. ML and TF activity also causes damage to a country's national security and reputation and has both direct and indirect impact on a nation's economy. Box 1 sets out examples of consequences of money laundering, to assist those carrying out ML/TF risk assessments to reach conclusions about the relative importance of each identified risk.

Box 1. Examples of Consequences of Money Laundering

- | | |
|---|---|
| • Losses to the victims and gains to the perpetrator | • Higher capital in-flows |
| • Distortion of consumption | • Changes in foreign direct investment |
| • Distortion of investment and savings | • Risks for financial sector solvency and liquidity |
| • Artificial increase in prices | • Profits for the financial sector |
| • Unfair competition | • Financial sector reputation |
| • Changes in imports and exports | • Illegal business contaminates legal |
| • Effects growth rates | • Distorts economic statistics |
| • Effects on output, income and employment | • Corruption and bribery |
| • Lower public sector revenues | • Increases crime |
| • Threatens privatisation | • Undermines political institutions |
| • Changes demand for money, FX-rates and interest rates | • Undermines foreign policy goals |
| • Increases in FX-rate and Interest rate volatility | • Increases terrorism |
| • Greater availability of credit | |

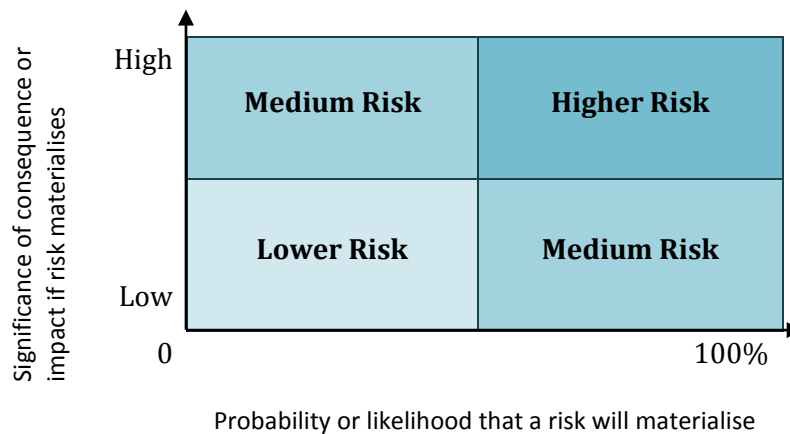
Source: Unger *et al.* (2006). The original source refers to *effects* – however, the term *consequences* as used in this table is consistent with the approach taken in this guidance.

56. A particular challenge especially when using more formal techniques is that ML/TF risks are inherently difficult to describe or measure in quantifiable or numerical terms. It is therefore important to remember that *risk* as we have discussed it in this guidance is a combination of threats, vulnerabilities along with consequences. If the level of risk of the individual risks can be examined according to their consequences or impact and the likelihood of their materialising, then a rough

²³ See FATF (2010), Annex C on “Crime and Terrorism Harm Framework”.

estimate of risk level may be obtained. A very simple matrix as applied to a specific risk might be as shown in Figure 3.²⁴

Figure 3. Examples of a Risk Analysis Matrix



4.3 Third stage: evaluation

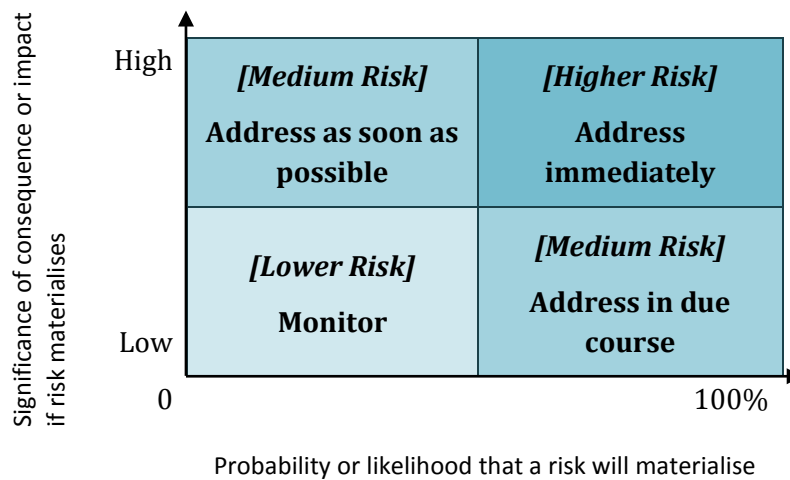
57. The last stage of risk assessment is evaluation. It involves taking the results found during the analysis process to determine priorities for addressing the risks, taking into account the purpose established at the beginning of the assessment process. These priorities can contribute to development of a strategy for their mitigation. As indicated in the introduction, this guidance does not attempt to provide a full explanation of this step of the process. For the sake of completeness however, some general details are set out here.

58. Depending on the source, there are a number of methods for addressing (or “controlling”) risk, including prevention (or avoidance), mitigation (or reduction), acceptance or contingency planning. In the context of ML/TF risk and the risk-based approach, the most relevant of these methods are prevention (*e.g.*, prohibiting certain products, services, or activities) and risk mitigation (or reduction). The role of evaluating levels of ML/TF risk therefore normally leads to the development of a strategy for addressing the risks. Working from the example in the last section, the evaluation of risk levels for each of the analysed risks could result in courses of action as illustrated in Figure 4²⁵, which is provided as a simple example of how the evaluation process might proceed at this stage:

²⁴ This example is adapted from UNODC (2010). Note: This example is intended to give a general idea of the thought process at this stage and is not meant to prescribe a particular approach. In some cases, a more detailed matrix might be used in order to indicate a broader range of levels of risk. For example, probability of likelihood could use a 5-step descriptive scale such as *Very likely / Likely / Possible / Unlikely / Very unlikely*, and impact or consequence might be described using a 3 point scale such as *Major / Moderate / Minor*.

²⁵ This example is adapted from UNODC (2010). See previous footnote.

Figure 4. Examples of a Risk Evaluation Matrix



59. According to this example, higher levels of risk might require more immediate action to mitigate it; lower levels of risk might require lesser action or some other response (the example here indicates monitoring). Alternatively, higher levels of risk may indicate systemic or deeply entrenched risks which require a broader response over time. By their nature, such responses generally require consultation (within government and between government and industry, among others), policy development and the implementation of measures, all of which can take time. The example shown here has been kept deliberately simple in order to clearly show the range of decisions that might be appropriate in addressing different levels of risk. A comprehensive ML/TF risk assessment process carried out at the national level might use a more detailed matrix in order to encompass a wider range of potential actions. Also note that, other types of risk matrices than the examples given above or a list ranking of the risks may also work, but the basic principles of the concept of risk as discussed in this paper should be applied.

60. The prioritisation of ML and TF risks at the evaluation stage will assist in the challenge of allocating scarce resources to fund AML/CFT programmes and other public policy and safety efforts. In the budgeting process, it is important to identify and prioritise issues that require attention. The evaluation process helps the authorities make decisions about how best to utilise resources and set priorities for regulatory agencies and the criminal justice system.

61. From an AML/CFT context, countries should implement necessary measures (for example, the FATF standards) and allocate appropriate resources to mitigate the risks which they have identified. In fact, the risk-based approach allows countries to develop a more flexible set of measures in order to target their resources more effectively, including by applying preventive measures flexibly to the financial and other sectors. Based on the risks identified, measures should address how best to prevent the proceeds of crime and funds in support of terrorism from entering into these sectors. Measures to mitigate risk should also address the ways in which these actors can better detect and report this activity. From an operational and criminal justice perspective, measures should be in place to better detect, disrupt and punish those who are involved in this activity.

5. OUTCOME OF RISK ASSESSMENTS

62. The actual results of a risk assessment can take different forms. For the public authorities that are ultimately the main users of the assessment, there is often an expectation that some form of a written report will be produced, although this is not strictly speaking a requirement of Recommendation 1²⁶. If the assessment will be presented in report form, decisions on how it will be organised – along with the level of detail – are most usefully made early on the risk assessment process and normally relate directly to the purpose and scope of the assessment. For example, a ML/TF risk assessment with law enforcement or other operational services as the primary users might discuss risks according to the threats (actors and activities) that were the starting point of the assessment. For a report whose primary audience consists of regulators or the private sector, a discussion of the risks grouped according to vulnerability (sector, product, etc.) might be most useful.

63. Regardless of the form and presentation of the ML/TF risk assessment, it should ultimately allow public authorities to make a judgment on the levels of the risks and priorities for mitigating those risks. The policy response can then be made commensurate to the nature and level of the risks identified. It is therefore advisable that the risk assessment contain sufficient information about the source, nature, and extent of each risk to help indicate appropriate measures to mitigate the risk. Thus, the results of national ML/TF risk assessments can provide valuable input in the formulation or calibration of national AML/CFT policies and action plans. This policy decisions may ultimately affect a number of competent authorities and how they carry out their responsibilities (*e.g.*, how financial investigations are conducted). The results of ML/TF risk assessments may also help inform planning for technical assistance on AML/CFT matters by a broad range of donors and technical assistance providers.

Dissemination of assessments outcome

64. Once completed, authorities will have to consider how broadly the results of the risk assessment are to be disseminated amongst the various stakeholders. More specifically, Recommendation 1 requires countries to have mechanisms to provide appropriate information on the results of the risk assessments to all relevant competent authorities and self-regulatory bodies (SRBs), financial institutions and DNFBPs.

65. Some ML/TF risk assessments may be considered to contain too much sensitive information to disclose publicly or that they may draw too much attention to the shortcomings in the AML/CFT system of a country. Furthermore, some of the information shared during the course of the assessment could be subject to confidentiality requirements. Nonetheless, appropriate information from assessments should be made available to the private sector to assist it in addressing the current ML/TF risks and new and emerging threats. In certain countries, committees or working groups with vetted private sector representatives have been created to share and discuss risk

²⁶ Countries will, however, be expected to demonstrate the process, mechanism and information sources used, as well as their understanding of and how they are addressing the identified risks.

assessment information. More generally, it may be helpful to share information – at a minimum – on the main factors considered and the conclusions of the risk assessment process with the private sector. Where the sensitive nature of the information prevents the broad distribution of the full results from the risk assessment report, consideration can be given to circulating sanitised information or summaries, or at least providing information on the methodology used, the findings and the conclusions. This approach could, for example, apply to information provided to assessors in the context of an AML/CFT assessment.

66. A particular objective of a ML/TF risk assessment could be to provide information to the public in order to enhance the general understanding of government AML/CFT initiatives. A typical output of a national ML/TF risk assessment is generally a public document. One challenge to overcome is that some information within the national assessment may be derived from classified or law enforcement sensitive sources. As such, some countries produce a non-classified version for the public.

ANNEX I. ML/TF RISK FACTORS RELATING TO THREAT

As mentioned in the Guidance, having an understanding of the environment in which predicate offences are committed and the proceeds of crime are generated to identify their nature (and if possible the size or volume) is important in order to carry out an ML/TF risk assessment.

The following is a list of crime categories that may be useful in building a picture or estimate of ML/TF threats. This list is not exhaustive, and the individual categories should be viewed as examples and may be complemented in accordance with the purpose and scope of the assessment.

Consideration of all stages of ML

- Placement
- Layering
- Integration

Consideration of all stages of TF

- Raising / collecting funds
- Moving funds
- Using funds

Threat Factors²⁷

- Nature and extent of relevant domestic criminal activity (*i.e.*, predicate offences).
- Types of predicate offences.
- Amounts of proceeds of crime generated domestically.
- Physical cross-border in and outflows of proceeds of crime.
- Amounts of proceeds of crime generated abroad and laundered domestically.
- Sources, location, and concentration of criminal activity, including within illegal underground areas in the economy.
- Nature and extent of relevant domestic terrorist activity and terrorist groups.

²⁷ See section on the following page for a list of categories of proceeds of crime / criminal offences that may be useful in looking at threat factors.

- Nature and extent of terrorist activities and groups in neighbouring countries, regions, or sub-regions.

The following is a list of criminal activities organised into categories and sub-categories that may also be useful in building a picture or estimate of threat (in the proceeds of crime environment). This list is not exhaustive, and the individual categories and subcategories should be viewed as examples.

Predicate Crime Categories for ML Crime Categories and Sub-Categories [Source: IMF]

Participation in an organised criminal group & racketeering

- Sophisticated organisations (*e.g.*, mafia, yakuza)
- Drug organisations
- Motorcycle gangs
- Street gangs
- Other

Terrorism and terrorist financing

- Raising funds from criminal activities
- Raising funds from "legal" or apparently lawful activities
 - Willing Donors using "Legal" Fundraising (*e.g.*, NPOs)
 - Deceptive Use of "Legal" Fundraising (*e.g.*, NPOs, donors unaware of TF use)
 - Donated from legal income (*e.g.*, salaries & profits)
- Other

Trafficking in human beings and migrant smuggling

- Trafficking (involuntary)
 - Inwards
 - Outwards
- Migrant smuggling (voluntary)
 - Inwards
 - Outwards
- Other

Sexual exploitation, including sexual exploitation of children

- General - unclassified
- Illegal prostitution
- Sexual slavery
- Procuring sexual activity with minors

- Selling/distributing illegal pornographic material
- Selling/distributing illegal pornographic material involving minors
- Other

Illicit trafficking in narcotic drugs and psychotropic substances

- Cocaine
- Marijuana/Cannabis
- LSD
- Ecstasy
- Meth/Amphetamines
- Heroin/Morphine/Opium
- "Magic" mushrooms
- Other

Illicit arms trafficking

- Small arms/guns
- Light weapons
- Larger Military hardware
- Ammunition
- Weapons of mass destruction
- Other

Illicit trafficking in stolen and other goods

- Stolen goods (NB: only to extent not captured under *e.g.*, theft)
- Gems
- Precious metals
- Radioactive materials
- Cultural goods
- Other

Corruption and bribery

- Bribery - major
 - Friendly GST/tax assessments
 - Avoiding investigation/prosecution
 - Procurement contracts
 - Permits/permissions/licenses
 - Other
- Graft - minor
 - Police
 - Traffic Police

National Money Laundering and Terrorist Financing Risk Assessment

FATF Guidance

- Customs Officers
- Licensing/Permit officials
- Other
- Embezzlement/misappropriation (theft)
 - Central/federal government
 - Local/state/county etc. government
- Bribery of private sector
- Bribery of foreign officials
- Bribery or embezzlement - international organisations
- Illegal lobbying and political campaign financing
- Other

Fraud

- Against government - General
- Against government - VAT/GST fraud
- Embezzlement/misappropriation (excluding from government by officials)
- Lending fraud (*e.g.*, mortgage fraud)
- Payment instrument fraud (*e.g.*, credit card, check fraud)
- Insurance fraud
- Healthcare fraud
- Benefit fraud
- Vendor, supplier & procurement fraud
- Confidence tricks/scams
- False billing/invoicing
- Cyber & Internet selling frauds (*e.g.*, “phishing”)
- Investment frauds (*e.g.*, Ponzi & pyramid schemes)
- Other fraud

Counterfeiting currency

- Local currency
- Foreign currency
- Other

Counterfeiting and piracy of products

- Illegal parallel imported products
- Patents/copyright/trademark infringement
- Clothing and shoes
- Accessories: bags/sunglasses/watches etc.
- Books

- Information technology
- CDs/DVDs, etc.
- Cigarettes
- Foodstuffs
- White ware & other electricals
- Pharmaceuticals
- Of collectibles (*e.g.*, wine, antiquities)
- Software
- Other

Environmental crime

- Illegal fishing
- Illegal logging
- Illegal dumping/polluting
- Illegal mining
- Other illegal extraction
- Illegal trading in endangered species (CITES)
- Illegal construction
- Other

Murder, grievous bodily injury

- Murder - for hire/contract killing
- Murder - motive is profit (*e.g.*, insurance claim)
- Grievous bodily injury- for hire or to derive funds or assets
- Other

Kidnapping, illegal restraint, and hostage taking

- Kidnapping/abduction for profit
- Hostage taking for ransoms
- Other

Robbery or theft

- Burglary - commercial
- Burglary - domestic/residential
- Theft/stealing/larceny
- Theft of motor vehicles (including car-jacking)
- Theft from motor vehicles
- Shoplifting
- Pick pocketing
- Bank robbery

- Pilfering/embezzlement (theft by employee)
- Robbery/mugging (including armed robbery)
- Cyber theft (*e.g.*, transferring bank balances through illegal account access)
- Other

Smuggling

- Prohibited imports
- Cigarettes
- Alcohol
- Cash smuggling of "clean" money (including dirty money would be double counting)
- Foodstuffs
- Prohibited exports
- Fuel
- Other

Extortion

- Blackmail
- Protection money/rackets
- Other

Forgery

- Of financial assets
- Philatelic forgery
- Of other documents
- Fake passports
- Fake ID/driver licenses
- Of art
- Other

Piracy (i.e., maritime)

- Theft from piracy
- Extortion or ransoms from piracy
- Other

Insider trading and market manipulation

- Insider trading
- Traded markets - market manipulation
- Anti-trust/cartel or anti-competition violations
- Boiler room scams
- Other

Tax & excise evasion

- Personal income tax
- Withholding tax
- Corporate income tax
- On illegal income sources
- Sales/turnover tax, VAT
- Customs/excise under invoicing - exports
- Customs/excise under invoicing - imports
- Customs/excise false declaration of quantity & product
- Sprints, tobacco, fuel excise evasions
- Gaming machine taxes and excise evasions
- Excise evasions related to counterfeit and piracy of products
- Other excise evasions
- Departure taxes & fees
- Death & estate duties
- Stamp Duty
- Capital gains taxes
- Real estate rental etc. taxes
- Informal sector
- Illegal transfer pricing
- Other

Illegal gambling

- Illegal lottery
- Illegal betting/bookmaking
- Illegal gambling houses/casinos
- Illegal online gambling
- Other

Money laundering

- Of foreign proceeds of crime

Other Proceeds Generating Crimes

- Computer crime
- Illegal trading of goods and services
 - Alcohol and tobacco
 - Pharmaceuticals, including internet pharmacy
 - Anabolic steroids
 - Party and other "non-narcotic" drugs

- Antiquities
- Illegal carrying out of a regulated/licensed business
 - Loan sharking/illegal lending
 - Illegal remittance activity
 - Illegal/prohibited FX dealing or money changing
 - Other illegal/prohibited financial services
 - Illegal professional services (*e.g.*, accounting, legal etc.)
 - Illegal health related services (*e.g.*, abortions, dentistry, donor tissue operations and trading etc.)

ANNEX II. ML/TF RISK FACTORS RELATED TO VULNERABILITIES

In order to understand the ML/TF risks facing a country, the relevant vulnerabilities need to be identified. This annex contains a longer list of examples of factors that may be considered at this stage of the ML/TF risk assessment to help identify relevant vulnerabilities. They have been generally arranged according to the analytical framework known as “PESTEL” (an acronym based on the first letters of the major categories: political, economic, social technological, environmental and legislative). This list is neither exhaustive nor binding, nor would these factors apply in every country’s ML/TF risk assessment and they should be applied in the context of each country²⁸.

Political factors

- Structure of the political system
- Stability of the present government
- Level of political commitment for AML/CFT programmes
- Level of political commitment to fighting crime
- Unaddressed history of terrorism financing activity
- Prevalence of organised crime, especially if involved in illicit drug production, illicit drug trafficking, kidnapping for ransom, extortion, intellectual property crime
- Presence of illicit small arms trade
- Prevalence of smuggling networks
- Presence of individuals, groups or organisations that support or promote violent extremism
- Weak government reach in some areas of the country, particularly border areas; porous borders
- High levels of corruption
- Adequacy of human, financial, and other resources of competent authorities
 - Inadequate resources
 - ML/TF not a national priority
 - No ML/TF risk assessment conducted by the authorities
 - Reluctance to acknowledge ML/TF risk
 - Lack of specialised training
 - Lack of commitment of financial sector, including low levels of reporting and/or lack of quality of STRs

²⁸ Some of the examples are taken from UNODC (2010).

- Financial sector not sufficiently concerned or incentivised regarding vulnerability to ML-related reputational risk
- Requirements of AML/CFT regime not well understood or implemented by financial institutions and DNFBPs
- Inadequate resources allocated to regulation of NPOs, given the risk level identified
- Inadequate resources allocated to address the issues on identify beneficial owners of foundations, associations and other similar entities, such as trusts
- Effectiveness of operations of competent authorities
 - Authorities' capabilities to suppress crime generally, and predicate offences to ML/TF specifically
 - Systemic weaknesses in law enforcement, and in authorities' efforts to counter crime generally, in particular ML/TF
 - Limited or non-existent ability of intelligence and law enforcement engaged in combating ML or TF to use financial information in their investigations
 - Inadequate co-ordination and information-sharing among law enforcement and intelligence agencies involved in combating ML/TF
 - Inadequate co-ordination among national authorities involved in combating ML/TF
 - Significant differences in procedure among competent authorities responsible for combating ML/TF
 - Lack of capabilities of financial intelligence unit (FIU) to process the reports that it receives
 - Lack of capabilities of law enforcement authorities (LEAs) to suppress ML or TF, which might result in ML or TF not being detected or investigated adequately
 - Lack of inter-agency cooperation that impedes AML/CFT processes and operations
 - Lack of capabilities of the prosecutors, the judiciary, and the prison system to deal with ML or TF related crimes, including weaknesses in the law, and other weaknesses that mean that offenders are not prosecuted, convicted, or sanctioned adequately or deprived of their assets or funds
 - Weaknesses in the authorities' ability to gather and share information due to a lack of capacity or legal privilege

- Inability to obtain convictions for ML/TF and related offences
- Lack of an operational FIU or FIU ineffective; inability or lack of capacity to examine STRs
- Lack of engagement or reluctance to engage regionally or internationally on AML/CFT issues, including on requests for assistance
- Ineffective border controls
- Border and immigration officials lack access to INTERPOL I-24/7 global police communication system
- Weak cash courier control at border points
- Weak AML/CFT oversight
- Government does not conduct regular reviews of terrorism financing risk in its NPO sector

Economic factors

- The type of economic system
- The amount of regulation within the economy
- Average earnings of the population
- Currency exchange rates
- Cost of services
- Size of the financial services industry
- Large, complex economy, or both (perhaps making it easier for ML/TF operations to go unnoticed)
- General opacity of the financial system
- Composition of the financial services industry²⁹
 - Products, services, and transactions
 - basic information on sectors or products
 - existence of those that facilitate speedy or anonymous transactions
 - cash transactions and cross-border funds transfers
 - delivery channels
 - existence of high-risk correspondent relationships between banks

²⁹ See also the list of financial institutions and services in later in this Annex.

- existence of measures to facilitate fiscal optimisation by non-residents (tax haven)
- Customer
 - types and ranges of customers (*i.e.*, entities, persons, etc.)
 - nature of business relationships
 - existence of higher risk customers
 - adherence to regulatory provisions applicable to customers
 - adherence to any restrictions on customer transactions
- Geographic
 - business and customer base in specific geographic areas
 - non-residents
 - customers from geographic area of concerns
 - adherence to any requirements in other countries
 - trans-national or cross-border movements of funds
- Ownership/ control of financial institutions and requirements concerning the identification of beneficial owners that are non-residents
- Corporate governance arrangements in financial institutions and the wider economy
- Nature and role of legal persons and legal arrangements in the economy
- Nature, existence, and size of sectors for legal persons and legal arrangements
- Nature of payment systems and the prevalence of cash-based transactions
- Cash-based economy with large informal sector; high percentage of cash outside legitimate banking system, especially relative to comparable countries
- Strict application of financial institution secrecy and other secrecy – including professional secrecy
- Geographical spread of financial industry's operations and customers
- Economic ties with jurisdictions at high risk of experiencing terrorism, political instability, or both
- Presence of NPOs active in overseas conflict zones or in countries or regions known to have a concentration of terrorist activity

- Presence of NPOs raising funds for recipients in a third country which are part of an organisational structure that engages in violent or paramilitary activities
- Opaque relations between grantees and NPOs disbursing funds or resources to grantees, *e.g.*, grantees are not required to disclose to the NPO how funds are used; no written grant agreement; NPO does not perform grantee due diligence, or due diligence is random and inconsistent; NPOs may disburse large sums for unspecified projects selected by the grantee.
- Effectiveness of financial institutions and DNFBPs in implementing the AML/CFT obligations or control measures
 - Customer due diligence
 - Ongoing due diligence, including transaction monitoring
 - Reporting measures currently performed
 - Internal controls
 - Record-keeping

Social factors

- The demographics of the society
- Extent of social inclusiveness
- Significant population shifts
- The ethnic diversity of the population
- Cultural factors, and the nature of civil society
- Areas of social, ethnic or political conflict
- Cultural immigrant, emigrant or religious ties with jurisdictions at high risk of experiencing terrorism, political instability, or both
- Low level of consultation / co-operation between government and financial sector
- Affiliates of banks circumvent international prohibitions that screen transactions for terrorists, drug traffickers, rogue jurisdictions and other wrongdoers
- Bank personnel not required to routinely share information among affiliates to strengthen coordination
- Requirements of AML/CFT regime not well understood or implemented by financial institutions and DNFBPs

Technological factors

- Use of transportation
- New communication methods

- The use of technology in money transfer
- Introduction and use of new payment methods

Environmental and geographical factors³⁰

- Global environmental factors such as availability of water, global warming, etc.
- The use and re-use of resources
- Impact of the local environment on crime such as housing, security etc.
- Impact of environmental legislation

Legislative factors

- Criminal justice system and legal environment
- Ease with which new legislation can be passed
- Review process for current legislation
- Impact of international standards on national legislation
- Strengths and weaknesses in legislation combating serious and organised crime
- Strengths and weaknesses in current AML/CFT legislation
 - AML/CFT preventive controls, including AML/CFT specific supervision and monitoring, that collectively do not deter ML or TF nor result in it being detected if it does occur
 - AML/CFT cross-border controls and international cooperation
 - Jurisdiction not a party to the International Convention for the Suppression of the Financing of Terrorism, the United Nations Convention against Transnational Organised Crime and its Protocols, and/or the United Nations Convention against Corruption
 - Adherence to international standards or conventions applicable to the specific sector or product
 - ML/TF not criminalised or inadequately criminalised
 - Incomplete coverage of predicate offences to ML
 - ML/TF not criminalised as a standalone offence
 - TF not a predicate offence to ML offence
 - TF not criminalised unless linked to a specific terrorist act
 - TF only criminalised in relation to the treaty-based offences

³⁰ Certain major categories provided in this example may not be relevant in all ML/TF assessments.

- No measures or inadequate measures to freeze without delay terrorist funds and assets
- Freezing of terrorist funds does not extend to other terrorist assets
- No legislation denying safe haven to those who assist or commit terrorist acts (laws on modalities of inter-State cooperation, extradition, mutual legal assistance, transfer of criminal proceedings, etc.)
- Government has not reviewed its own policies, legislation and other tools in respect of terrorism financing risk in the NPO sector and taken steps to address shortfalls
- Regulation of charitable donations does not cover overseas donations
- Lack of early warning arrangements with other jurisdictions on CFT
- Financial sector not prohibited from conducting relationships with shell banks or shell companies
- Adequacy of AML controls
 - Customer due diligence
 - Ongoing due diligence including transaction monitoring
 - Reporting measures currently performed
 - Internal controls
 - Record keeping
 - Lack of regulation on beneficial ownership
- Lack of guidance to relevant authorities on beneficial ownership
- Limited or absence of risk-based approach guidance on AML/CFT provided by regulatory, oversight and supervisory authorities
- Limited regulation of money or value transfer systems
- Entities not registered and size of sector unknown
- No system of registering or licensing service providers; difficult to take enforcement action and thereby to formalise flows of funds

National Money Laundering and Terrorist Financing Risk Assessment

FATF Guidance

- Any non AML/CFT controls that apply to entities that can be abused for ML or TF, including general supervision or monitoring
- Any non-AML/CFT related cross-border controls, including general border security
- Extent and efficacy of compliance audits
- Enforceability of rules or guidance
- Existence of a regulator or supervisor
- Links with other financial intermediaries
- Legal or other constraints on products, services, transactions
- Coverage or requirements in other countries

The following table provides a generic list of entities /sectors that may be useful in building a list of the ML/TF vulnerabilities that can be exploited in regulated entities. In particular, it may be worth using such a list to think about vulnerabilities in the context of types of products and services offered by each type of institution or firm and the adequacy of their AML/CFT controls. This list is not exhaustive, and the individual sectors / entities included here should be viewed as examples.

Table 1. **Institution and firm categories by sectors**

Sector	Categories of institutions and firms
Banks and credit institutions	<i>All banks or commercial banks (including: foreign banks, government-owned banks, merchant banks, special purpose banks)</i>
	<i>All offshore banks (offering services exclusively to non-residents)</i>
	<i>Building societies, cooperatives and credit unions</i>
	<i>Central bank WITHOUT retail base</i>
	<i>Central bank WITH retail base</i>
	<i>Finance companies</i>
	<i>Savings institutions (including postal savings service)</i>
	<i>Microfinance deposit takers</i>
	<i>Merchant banks</i>
	<i>Shell banks</i>
Securities industry	<i>Advisers</i>
	<i>Fund and asset managers (including mutual funds)</i>
	<i>Futures (including commodities) & derivatives brokers and dealers</i>
	<i>Markets, registries & exchanges</i>
	<i>Securities firms (brokers, dealers and other companies)</i>
	<i>Superannuation and pension companies</i>

Sector	Categories of institutions and firms
	<i>Other</i>
Insurance industry	<i>Life insurance agents and brokers</i>
	<i>Non-life insurance agents and brokers</i>
	<i>Non-life insurance companies</i>
	<i>Offshore insurers</i>
	<i>Superannuation and pension companies</i>
	<i>Other Insurance</i>
Money services businesses (MSBs)	<i>Card issuers/E-payment (credit, debit, E-cash/money etc.)</i>
	<i>Check issuers and cashers</i>
	<i>Foreign exchange dealers (including bureaux de change and money changers)</i>
	<i>Money remitters and transfer agents (including any postal service that offers this service)</i>
	<i>Undertaking of bill payment business</i>
	<i>All (Other) MSBs</i>
Other financial institutions	<i>Hire purchase companies</i>
	<i>Mortgage providers</i>
	<i>Other lenders</i>
	<i>Other specialist financial institutions (such as development FIs)</i>
	<i>Pawnshops (if they "lend")</i>
	<i>Providers of deposit boxes</i>
	<i>Specialised financial institutions</i>
	<i>Cash handling firms</i>
DNFBPs	<i>Accountants</i>
	<i>Auditors</i>
	<i>Casinos</i>
	<i>Dealers in precious metals and stones</i>
	<i>Lawyers (including barristers, solicitors, and other legal professionals)</i>
	<i>Notaries</i>
	<i>Real estate agents (including licensed conveyancers)</i>
	<i>Trust and company service providers (including: company formation agents)</i>
	<i>All (Other) DNFBPs</i>

National Money Laundering and Terrorist Financing Risk Assessment

FATF Guidance

Sector	Categories of institutions and firms
Other entities	<i>Advisors, including tax and financial</i>
	<i>Bookmakers, betting, gaming & lotteries</i>
	<i>Motor vehicle retailers</i>
	<i>Boat charterers, sellers, and re-sellers</i>
	<i>Aircraft charterers, sellers, and re-sellers</i>
	<i>Art and antique dealers</i>
	<i>Auction houses</i>
	<i>Other dealers and traders in high value goods</i>
	<i>Pawnshops</i>
	<i>Travel Agents</i>
	<i>Convenience, grocery, liquor stores</i>
	<i>Laundromats, car washes, parking businesses</i>
	<i>Other cash intensive businesses</i>
	<i>Construction companies</i>
	<i>Customs agencies and brokers</i>
	<i>Mail and courier companies</i>
	<i>Hotels</i>
	<i>Restaurants and bars</i>
	<i>Mining, logging, and other extractive industry companies</i>
	<i>Other</i>
Legal persons	<i>Bodies corporate</i>
	<i>Registered companies *</i>
	<i>Public companies *</i>
	<i>Companies that have issued bearer shares *</i>
	<i>Companies owned or controlled by non-residents *</i>
	<i>International or (foreign) business companies or corporations *</i>
	<i>Other types of company *</i>
	<i>Foundations</i>
	<i>Anstalt</i>
	<i>Partnerships</i>
	<i>Associations</i>
	<i>Similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property</i>
	<i>All legal persons (other than companies) that are owned or controlled by non-residents including branches or offices of foreign legal persons authorised to operate in the</i>

Sector	Categories of institutions and firms
	<i>jurisdiction *</i>
Legal arrangements	<i>Express trusts (i.e., with a written deed of trust)</i>
	<i>Fiducie</i>
	<i>Treuhand</i>
	<i>Fideicomiso</i>
	<i>Other similar legal arrangements</i>
	<i>International Trusts*</i>
	<i>All legal arrangements established or controlled by non-residents*</i>
Non-profit organisations (NPOs)	<i>NPOs - registered or licensed</i>
	<i>NPOs - not registered or licensed</i>
	<i>All NPOs established or controlled by non-residents*</i>

Table note

* These are memorandum items only as they should already appear in other categories.

ANNEX III. EXAMPLES OF NATIONAL-LEVEL ASSESSMENTS

This annex shares countries' efforts to assess ML/FT risks at the national level (whether focusing on threats, vulnerabilities, or both). These are presented as examples only. At the time of the publication of this guidance, the individual efforts had not been assessed for compliance with Recommendation 1; therefore, their presentation here should not be considered as an endorsement by FATF.

Australia

FATF Guidance on risk assessments – project group

Australian National Threat Assessment on Money Laundering 2011 (NTA)

Australia adopted a 'top-down' approach in 2011, producing the country's first National Threat Assessment (NTA). The NTA was a key element of the organised crime strategic framework the Australian Government adopted in 2009. The NTA involved only government agencies. AUSTRAC, the national FIU and AML/CFT regulator (*i.e.*, supervisor), led the project with primary input coming from five national government agencies (policy, revenue, law enforcement and border protection) and one state-based law enforcement intelligence agency. Incidental information came from a handful of national and state agencies on particular issues as required.

A two-tiered system was established to coordinate input and provide direction across agencies. A steering committee of senior officials was formed to provide guidance and governance to the assessment and resolve any issues that arose. The level below involved a working group of intelligence analysts, law enforcement officers and policy advisers to collect and analyse information, and work with the FIU on drafting the assessment. Once approved by the steering committee and the head of the FIU, the assessment was submitted to the heads of operational agencies in national government (comprising law enforcement, the FIU, border protection and regulatory agencies).

The NTA draws together information from across key government agencies to form a consolidated picture of the Australian money laundering environment. It is focused on the Australian environment and what Australian agencies and experts see as the current and emerging threats. Close attention is paid to money laundering associated with higher risk organised crime activity. It also examines high-risk countries that influence the Australian environment. International experience is drawn upon where required to amplify an aspect of the Australian situation, or to help address gaps in the Australian picture.

Information sources are primarily intelligence based. Current intelligence insights, operational cases, and expert views inform the discussion of current and projected money laundering activity. Limited statistical data, particularly the financial value tied to money laundering activity, meant the NTA is largely a qualitative threat assessment.

Threat matrix

The NTA modified the ‘features’ adopted in the FATF *Global Money Laundering and Terrorist Financing Threat Assessment* (GTA)³¹, using terminology about channels, sectors and vulnerable individuals (industry insiders and PEPS) that would be readily understood by an Australian audience. Assessment of each area took into account:

- Government measures (law and regulation, law enforcement and regulatory activity, specialist intelligence work where relevant)
- Current intelligence picture
- Drivers and enablers (adopted from the GTA)
- Gaps in intelligence, information and measures
- Threat assessment with a three-year forecast where possible

To overcome the limitations faced in trying to apply conventional threat analysis (intent x capability = threat) to money laundering, a threat matrix (see Table 2 below) was customised for Australia’s circumstances to rank relative levels of threat. It assessed threats and vulnerabilities in terms of:

- **Accessibility** or availability of services that might be misused for ML – scale from easy, moderate to difficult (the easier to access, the higher the threat)
- **Ease of use** – same scale as above
- **Deterrence** – scale of significant, limited to weaker (significant = measures reasonably effective at lowering threat of ML)
- **Detection** – scale of likely (detection of ML), limited to difficult (detection is unlikely due to intelligence gaps, opaque and complex services)
- **Criminal intent** to launder (a function of the above categories and assessments of current and emerging organised crime behaviour and trends)

Weightings for the scales used above were developed to produce rough scores of levels of threat, from undetermined to low, through to medium and high. Scoring was not adopted as a strict science, but rather as a starting point to stimulate expert discussion among the involved agencies. Threat scores were also used in conjunction with the analysis of each area, to test intelligence judgements and, vice versa, test the validity of the scoring system itself.

³¹ FATF (2010).

National Money Laundering and Terrorist Financing Risk Assessment

FATF Guidance

Table 2. Australian Threat Matrix

Threat factors	Low threat	Medium threat	High threat
ACCESSIBILITY e.g. accessibility and relative cost	Difficult Difficult to access and/or may cost more than other options.	Moderate Reasonably accessible and/or a financially viable option.	Easy Widely accessible and available via a number of means and/or relatively low-cost.
EASE OF USE e.g. knowledge and/or technical expertise and support required	Difficult Requires more planning, knowledge and/or technical expertise than other options.	Moderate Requires moderate levels of planning, knowledge and/or technical expertise.	Easy Relatively easy to abuse; little planning, knowledge and/or technical expertise required compared to other options.
DETERRENCE e.g. existence of AML and/or other barriers to abuse	Significant Deterrence measures and controls exist and are reasonably effective at deterring money laundering.	Limited Deterrence measures and controls have some effect in deterring criminal abuse of the service.	Weaker There are limited or no measures and controls in place, or they are not working as intended.
DETECTION e.g. ability for money laundering to be identified and reported to authorities	Likely A range of money laundering methods is visible and likely to be detected.	Limited Some money laundering methods may be visible but limited reporting, high volumes of funds flows and/or effective evasion techniques limits detection.	Difficult Detection is difficult and there are few financial or other indicators of suspicious activity.
INTENT e.g. perceived attractiveness of money laundering through this mechanism	Low Perceived as relatively unattractive and/or insecure.	Moderate Perceived as moderately attractive and/or fairly secure.	High Perceived as attractive and/or secure.

High-risk countries³²

To improve the capacity of Australian authorities to assess and weigh-up the ML threats/risks foreign countries pose to Australia, the NTA developed a high-risk country matrix. It essentially is a checklist of the main indicators and attributes which influence a country's risk profile, as a source, destination or conduit for laundered funds. A copy of the matrix table, sanitised with countries removed, is attached to this paper. It involved a larger set of indicators (listed below) than the

³² Even though the NTA is a threat assessment, the term 'high-risk countries' was used due to its commonplace usage in official circles.

threat matrix above. Many of the risk indicators are drawn from FATF guidance. Numerical weightings or scoring were not used with the matrix, but the format lends itself to such an approach if required.

For the sake of clarity, the NTA divided high-risk countries into two broad crime types: organised/transnational crime and offshore tax evasion. Although the boundary between these two categories is blurred and some countries appear in both groups, this approach helped to sift through a long list of countries. It also provided a sharper focus on the nature of illicit funds flows involving different countries, than would have been the case if they had all been lumped under the 'high-risk' tag.

High-risk country indicators

- Variable regulations, such as lax AML/CFT provisions, weak regulation of business registration, financial markets and foreign currency exchange
- Preferential tax regimes identified by the OECD
- Strong secrecy provisions in banking and finance
- High volume of non-bank international remittances
- Regional or global financial centres
- Free-trade or special economic zones
- Source countries for illicit commodities and services
- Transit countries for illicit commodities and services
- Low tax on foreign income
- Ability to easily create complex legal entities to hide beneficial ownership of assets
- Countries with perceived high-level corruption
- Countries embroiled in high-level internal or external conflict
- Patterns of evasion of exchange controls by legitimate businesses
- Limited asset forfeiture and seizure powers
- Weak law enforcement and border control capabilities
- Large parallel or black market economies
- Cash intensive economies
- Countries with no extradition treaty with Australia
- Jurisdictions that are either a place of residence for members of a criminal network or where members of a criminal network have strong familial or cultural ties, or both
- Jurisdictions where criminal entities can obtain dual nationality

Approach and lessons learnt

Since it was Australia's first NTA, the intention was to involve a core of key government agencies in laying the foundations upon which subsequent national assessments could build. Wider involvement from industry and other government bodies at the national and state/territory level is something to be considered for future assessments.

A key lesson from the first NTA is that any decision to involve more partners or stakeholders should be made on the basis of the value of data, intelligence and expertise they can commit to an assessment. Relevant expertise and a guaranteed commitment of resources (staff and time) are essential for the successful completion of such a large exercise. The 'hidden cost' in time and staff in consulting and coordinating many stakeholders should not be underestimated.

The NTA examines only money laundering and excludes terrorism financing threats. Differences between ML and TF, limited cases in the Australian context and difficulties in managing highly sensitive intelligence were all seen as likely to create added problems for a complex assessment that was first of its kind in Australia and largely exploratory. As with the decision to limit the number of agencies involved, the NTA was seen as paving the way to undertake a TF assessment in the future.

The NTA originally included, in line with the GTA framework, harms analysis for each area under examination. Harms were later omitted to avoid any conceptual confusion as to whether the NTA was a *threat* assessment (harms or consequences excluded) or a *risk* assessment (harms and consequences included). The more important reason for the omission was due to the lack of available evidence of ML harms in Australia, beyond sustaining continued and expanded criminal activity. Overseas experience of ML harms was largely seen as not directly relevant or provable in the Australian context.

The Netherlands

In 2005, a study was conducted titled: "The Amounts and Effects of Money Laundering"³³. Its objective was to obtain better information on the amount, flows and effects of money laundering. The study was based on a quantitative method to estimate the amounts, flows and effects of money laundering. In addition, (extensive literature) research was carried out on definitions, typologies and growth effects. There was also an effort to identify forms of money laundering, typically existent in The Netherlands. The findings were mainly based on qualitative judgments but sometimes supported by quantitative data. The results of the study were used as input for policy formulation.

In 2011 a National Threat Assessment (NTA) was carried out in the Netherlands. The Ministry of Finance was leading the project and established a project plan which was submitted to and approved by the Financial Expertise Centre³⁴. The exercise commenced by interviewing all relevant stakeholders, including for example: financial sector, supervisory authorities, research institutes

³³ Unger *et al.* (2006).

³⁴ The Financial Expertise Centre (FEC) is a partnership between authorities that have supervisory, control, prosecution or investigation tasks in the financial sector and was founded to strengthen the integrity of the sector. Authorities involved in the FEC are: Dutch Central Bank, Financial Markets Authority, Public Prosecutor, Tax Authorities, Intelligence Services, National Police, Ministry of Justice and Ministry of Finance.

and law enforcement. Based on the outcome of these interviews, the project team identified a list of mayor topics/issues and organised several workshops to discuss the selected items. Participants in these workshops were policymakers, supervisory authorities, prosecutors, police and tax authorities. As a result of this series of workshops three mayor topics were identified and these became subject of an in depth research. The project team analysed and described cases and trends/developments on these items and made recommendations for further work on these issues. Finally, the report has been presented to the Ministry of Finance and the Ministry of Justice with the objective to translate the outcome of the NTA into national policy measures. Relevant information resulting from this process has been published or made available to relevant non-public bodies, but the NTA itself remained a classified document.

In 2012 the National Police Services Agency (KLPD) conducted a National Threat Overview focused on money laundering. The method used by the KLPD was the following: again the research was commenced by a series of interviews with stakeholders. These interviews served as a basis for an in depth research in criminal files and data systems. This resulted in a description of several methods of money laundering, characterisation of persons involved and consequences for the Dutch society. Finally, the National Threat Overview is addressing some general developments concerning money laundering in the future.

Switzerland: Example of a risk assessment used as the basis for applying low-risk exemptions

Switzerland has developed a risk assessment process as a basis for applying low risk exemptions. A working group was established from September 2009 to January 2010, which was composed of experts from the banking, insurance and non-banking sectors, auditors, law enforcement authorities and the financial regulator. The working group identified low-risk products for which the exemptions could apply. This work resulted in the adoption of regulation which establishes an ongoing risk assessment process.

On the basis of the aforementioned regulation, a committee of experts, established by FINMA, can authorise exemptions from CDD measures for customer relationships at the request of SROs or financial intermediaries if there is a proven low risk for money laundering. In order to get a decision from FINMA allowing a financial intermediary to benefit from an exemption, the requestor has to provide all elements necessary for FINMA to take this decision. FINMA then verifies if the regulatory conditions for an exemption are met, and in particular if the low risk is given on a case-by-case basis. To come to a decision, FINMA analyses every request separately and in detail. Different criteria are taken into consideration. FINMA examines whether the FATF has already considered the activity under the risk aspect. It examines if similar cases have already been subject to criminal or other enforcement measures. Finally, FINMA decides if the risk is low in the concrete case, but also if it will remain low if the circumstances would slightly change. Consideration is given to product, services, transactions as well as customer risk and to the legal environment, as well as to every other relevant characteristic of the activity, in order to decide whether the risk is low. FINMA has the legal obligation to publish its practice.

United States

In 2005, the United States initiated its first multi-agency money laundering threat assessment. Quantitative inputs included prosecution data from federal law enforcement agencies and suspicious transaction reporting via the financial intelligence unit. Qualitative inputs came from law enforcement and regulatory case studies with private sector reporting.

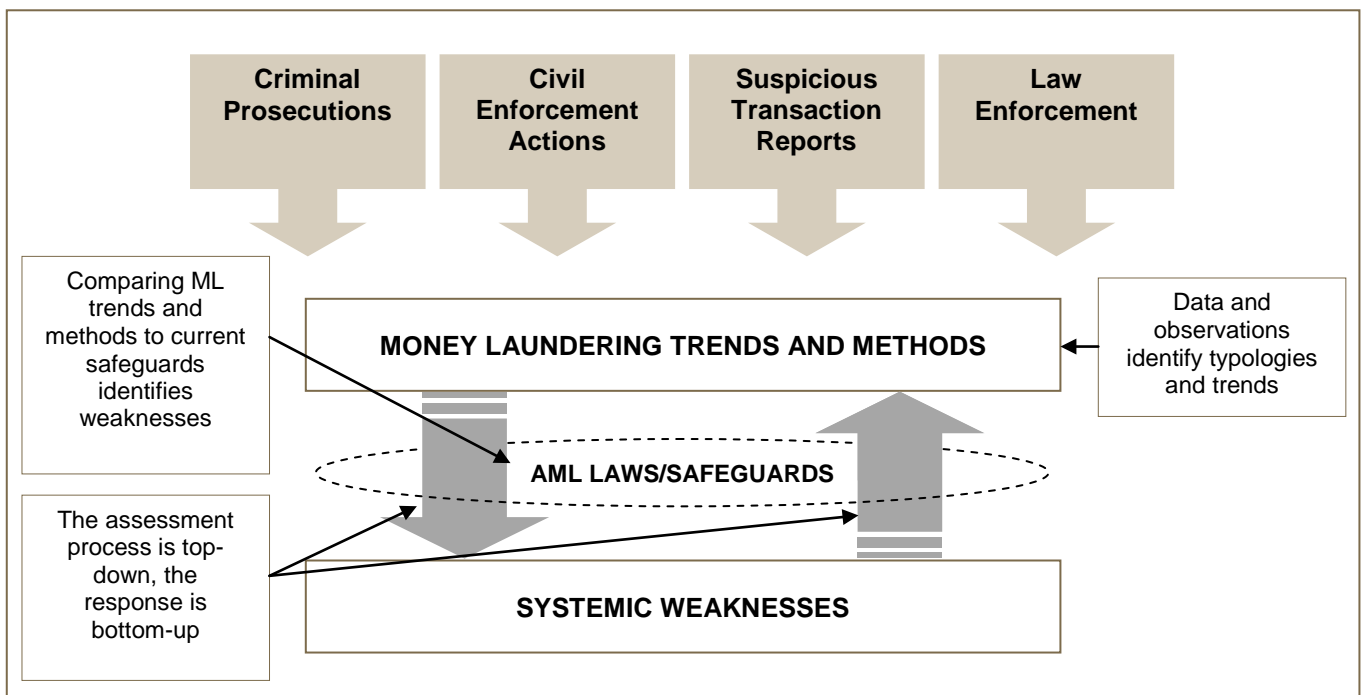
The 2005 *U.S. Money Laundering Threat Assessment*³⁵ was divided into the following sections: banking, money services businesses, (*i.e.*, money transmitters, cheque cashers, currency exchangers, money orders and stored value cards); online payment systems; informal value transfer systems; bulk cash smuggling; trade-based money laundering; insurance companies; shell companies and trusts; and casinos.

The project team made assumptions and observations about vulnerable sectors using the available information, considered whether adequate safeguards were in place to address the identified vulnerabilities and made a subjective determination about the residual threat.

This was a multi-agency process, including offices and agencies under the US Departments of Homeland Security, Justice and Treasury. Also participating was the Board of Governors of the Federal Reserve System and the United States Postal Inspection Service.

The available information was synthesised to form a qualitative assessment, which included, to the extent possible, the relative effectiveness of AML safeguards. In some cases, data was available to support subjective judgments regarding effectiveness (see Figure 5). Otherwise, the determinations were the result of broad intergovernmental discussion and analysis.

Figure 5. Flow chart depicting US money laundering assessment and strategy formation process



³⁵ Money Laundering Threat Assessment Working Group (U.S. Department of the Treasury, *et al.*) (2005).

ANNEX IV. SPECIFIC RISK ASSESSMENT METHODOLOGIES

The International Monetary Fund Staffs' ML/FT National Risk Assessment Methodology:

[www.fatf-gafi.org/media/fatf/documents/reports/Risk Assessment IMF.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Risk%20Assessment%20IMF.pdf)

The World Bank Risk Assessment Methodology

[www.fatf-gafi.org/media/fatf/documents/reports/Risk Assessment World Bank.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Risk%20Assessment%20World%20Bank.pdf)

BIBLIOGRAPHY

Relevant FATF material (all available at: www.fatf-gafi.org)

FATF (2012), *The FATF Forty Recommendations*, FATF, Paris.

FATF (2010), *Global Money Laundering and Terrorist Financing Threat Assessment*, FATF, Paris.

FATF (2008), *Money Laundering and Terrorist Financing Risk Assessment Strategies*, FATF, Paris.

FATF, (2007), *Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures*, FATF, Paris.

Country-level assessments of interest (available on line)

Australia:

AUSTRAC (2011), *Money laundering in Australia 2011*, Sydney,
www.austrac.gov.au/files/money_laundering_in_australia_2011.pdf

Netherlands:

Unger *et al.* (2006), *The Amounts and the Effects of Money Laundering*, Report for the Ministry of Finance, Amsterdam, www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2006/02/16/onderzoeksrapport-the-amounts-and-the-effects-of-money-laundering/witwassen-in-nederland-onderzoek-naar-criminele-geldstromen.pdf

New Zealand:

New Zealand Police (2010), *National Risk Assessment 2010*, Wellington,
www.justice.govt.nz/policy/criminal-justice/aml-cft/publications-and-consultation/20110308-NRA-2010-Primary-Document-FINAL.pdf

New Zealand Department of Internal Affairs (2011), *Internal Affairs AML / CFT Sector Risk Assessment*, Wellington, [www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf/\\$file/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf/$file/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf).

New Zealand Securities Commission (2011), *Sector Risk Assessment*, Wellington,
www.fma.govt.nz/media/186534/aml-cft-sector-risk-assessment.pdf.

Reserve Bank of New Zealand (2011), *Sector Risk Assessment*, Wellington,
www.rbnz.govt.nz/aml/4345201.pdf.

United States:

Money Laundering Threat Assessment Working Group (U.S. Department of the Treasury, *et al.*) (2005), *U.S. Money Laundering Threat Assessment*, U.S. Department of the Treasury, Washington, DC,
www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf

Other material

Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2004), *Enterprise Risk Management – Integrated Framework*, COSO, website: www.coso.org/erm-integratedframework.htm.

European Network and Information Security Agency (ENISA) (2006), *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment Methods and Tools*, Heraklion [Greece], website: www.enisa.europa.eu/activities/risk-management.

EUROPOL (2011), *Organised Crime Threat Assessment*, Europol, The Hague, www.europol.europa.eu/sites/default/files/publications/octa_2011_1.pdf.

The Institute of Risk Management et al. (2002), *A Risk Management Standard*, [United Kingdom], www.theirm.org/publications/PUstandard.html.

International Organisation for Standardisation (ISO) (2009a), *Risk Management – Principles and Guidelines* (ISO 31000:2009), ISO, Geneva, website: www.iso.org.

ISO (2009b), *Risk Management – Risk Assessment Techniques* (ISO 31010:2009), ISO, Geneva, website: www.iso.org.

ISO (2009c), *Risk Management – Vocabulary* (ISO Guide 73:2009), ISO, Geneva, website: www.iso.org.

Organisation for Security and Co-operation in Europe (OSCE) (2012), *OSCE Handbook on Data Collection in Support of Money Laundering and Terrorism Financing National Risk Assessment*, Vienna, www.osce.org/eea/96398.

Standards Australia and Standards New Zealand (2009), *Risk Management – Principles and Guidelines* (AS/NZS ISO 31000:2009), SAI Global, website: www.infostore.saiglobal.com/store.

Treasury Board of Canada (2001), *Integrated Risk Management Framework*, Ottawa, www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19422§ion=text.

United Nations Office on Drugs and Crime (UNODC) (2010), *Guidance on the preparation and use of serious and organised crime threat assessments* [“The SOCTA Handbook”], UNODC, Vienna, www.unodc.org/documents/afghanistan/Organized_Crime/SOCTA_Manual_2010.pdf.

U.S. Department of Homeland Security (2010), *DHS Risk Lexicon – 2010 Edition*, Washington DC, www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

EXHIBIT 23

Kim, Jane (USANYS) 4

From: Krouse, Michael (USANYS)
Sent: Friday, March 6, 2020 10:46 PM
To: Kim, Jane (USANYS) 4
Cc: Lake, Stephanie (USANYS); Lynch, Garrett (USANYS) [Contractor]
Subject: Re: Exhibit admission issues & commerzbank

The judge said we can put in parts that were redacted, so that's an option on redirect. Should we pick stuff, mark it, and offer?

Sent from my iPhone

> On Mar 6, 2020, at 10:02 PM, Kim, Jane (USANYS) 4 <JKim4@usa.doj.gov> wrote:

>

> We maybe should've kept this whole thing in (rather than redacting):

> <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FAT>

> F%20Recommendations%202012.pdf

>

> I think we should get in some of FATF's risk assessments and standards. Attaching 3 docs – haven't reviewed closely, but these might make sense. The SKN one didn't end up including specifics on the passports. We could offer that if one of their defense witnesses testifies (mainly Klingensmith).

>

> From: Lake, Stephanie (USANYS) <SLake@usa.doj.gov>

> Sent: Friday, March 6, 2020 9:45 PM

> To: Krouse, Michael (USANYS) <MKrouse@usa.doj.gov>; Kim, Jane (USANYS)

> 4 <JKim4@usa.doj.gov>; Lynch, Garrett (USANYS) [Contractor]

> <GLynch@usa.doj.gov>

> Subject: Exhibit admission issues & commerzbank

>

> I went through the transcripts to confirm that all of the exhibits we've noted as admitted were actually admitted. I found some issues. Not positive what the best way to fix is (aside from the first one, for which I'll just reach out to court reporters).

>

>

> 1) In the March 3 transcript (page 114), says Jane offered 910 – 907. Definitely a typo – should be 910-917.

>

> 2) March 3 (Kazerani) – transcript doesn't reflect 2021A as offered /admitted, although 2021A-T was.

>

> 3) March 4 (Iran) – transcript doesn't reflect 2104-T being offered / admitted.

>

> 4) March 5 (SDN/Knowledge of Sanctions) – it looks like the court never officially admitted 1103 after overruling the defense objection.

>

> Can we all talk briefly tomorrow morning about the Commerzbank thing?

> <GX 4[] high-risk-and-other-monit.pdf> <GX 4[] FATF Recommendations

> 2012.pdf> <GX 4[] National_ML_TF_Risk_Assessment.pdf>

EXHIBIT 24

Kim, Jane (USANYS) 4

From: Kim, Jane (USANYS) 4
Sent: Saturday, March 7, 2020 9:58 AM
To: 'Lynch, Garrett'; Lake, Stephanie (USANYS); Krouse, Michael (USANYS); Lynch, Garrett (USANYS) [Contractor]
Subject: Things to do

Banking testimony

- Peri re-direct (GL)
- Commerzbank production (SL)
- Commerzbank custodian (GL)
- Any FATF, Hyposwiss, or other docs we want to admit (SL and GL?)

Closing/Rebuttal (MK and JK)

Monday witnesses

- Payment chart (GL)
- Travel chart (SL)
- Follow the money chart (SL)

RTC – should we split up sections to argue or SL do you want to handle?

Defense case

- Letter re Parsi and Klingensmith (SL finishing)
- Defense exhibits/objections (maybe we should all do this together except Krouse)
- Defendant cross (GL)
- OFAC witness cross (JK)
- Character witness cross (SL)
- Unlikely Parsi and Klingensmith will testify, but MK is doing Klingensmith and SL do you still want to do Parsi?

Rule 29 (figure out if/when they file)

EXHIBIT 25

Kim, Jane (USANYS) 4

From: Lake, Stephanie (USANYS)
Sent: Saturday, March 7, 2020 10:48 AM
To: Milione, Shawn (USANYS) [Contractor]
Cc: Krouse, Michael (USANYS); Kim, Jane (USANYS) 4; Lynch, Garrett (USANYS) [Contractor]
Subject: GX 411
Attachments: Commerz OFAC disclosure.pdf

Hey Shawn,

Can you let me know when you think you'll have a chance to mark this GX 411? If you won't be in for a while and can tell me how to do it, I'm happy to do it myself!

Thanks!

Stephanie Lake
Assistant United States Attorney
Southern District of New York
One Saint Andrew's Plaza
New York, NY 10007
Tel: (212) 637-1066

EXHIBIT 25-1



NEW YORK BRANCH

Department of the Treasury
Office of Foreign Assets Control
1500 Pennsylvania Avenue NW
Washington DC 20220

Vinay Jepsal
2 World Financial Center, New York, NY 10281-1050
Telephone (212) 266-7200
Fax (212) 266-7235
vinay.jepsal@commerzbank.com

June 16, 2011

Re: Information Sharing – Stratus International Contracting Company

Dear Sir/Madam:

Commerzbank AG, New York Branch (CBNY) would like to share the following information with OFAC. On April 20, 2011 CBNY's AML transaction monitoring system generated an alert, which involved a transaction for USD 29,442,967.57 value April 4, 2011.

The transaction was originated by Banco Del Tesoro, CA Banco Universal Caracas for its client BT / Fideicomiso / Fondo Chino Venezolano in Caracas, Venezuela. The beneficiary of the payment was Stratus International Contracting Company ("Stratus"), a client of Hyposwiss Privatbank AG, Zurich.

As per standard procedure, CBNY initiated a request for information to the remitting bank Banco Del Tesoro, CA Banco Universal Caracas, Venezuela to obtain details on both entities and their relationship. In the interim, CBNY conducted further due diligence and noted the following regarding Stratus from its website:

- Stratus was founded in 1978 in Tehran, Iran
- Stratus International specializes in providing contracting services to infrastructure projects such as roads, railways, dams, tunnels, airports and buildings.
- Stratus is presently working on a 7000 Apartment Unit "New Ojeda" Housing Development Project in Venezuela

On May 12, 2011, CBNY received a response from the bank in Caracas indicating the following:

- Stratus's physical address is Gardenya Plaza 5, K:3 D:3 (Floor 3, Suite3) 34758 Atasehir, Istanbul, Turkey
- Stratus is registered in Istanbul, Turkey (copy of the registration attached)
- Stratus provides construction services in Turkey, Dubai and Venezuela
- The purpose of the payment is for the construction of a 7000 apartment unit project "Proyecto Urbanismo Nueva Ciudad Fabricio Ojeda, in Ciudad Ojeda, Estado Zulia, Venezuela (same address as listed on Stratus' website)

Although Stratus is not listed as an SDN, and the payment does not indicate any direct involvement of Iran or with Iran, due to conflicting information between the website and the response forwarded by the bank in Caracas, CBNY believes it appropriate to share this information with OFAC since Stratus may be an Iranian Company.

Chairman of the Supervisory Board: Klaus-Peter Müller
Board of Managing Directors: Martin Blessing (Chairman),
Frank Annuscheit, Markus Beumer, Achim Kassow, Jochen Klösges,
Michael Reuther, Stefan Schmittmann, Ulrich Sieber, Eric Strutz, Martin Zielke

Commerzbank Aktiengesellschaft, Frankfurt am Main
Registered Office: Frankfurt am Main Reg.No. 32000
VAT No. DE 114 103 514



NEW YORK BRANCH

Re: Information Sharing – Stratus International Contracting Company– Page 2

We have added Stratus into our sanctions filter to monitor any future payments. Please note that apart from this transaction, there have not been any other payments involving Stratus processed by CBNY to date.

The purpose of this letter is to report the good faith efforts of Commerzbank AG, New York Branch in complying with applicable OFAC requirements and voluntarily informing OFAC of any information received during its investigation into possible sanctions-related entities.

Should you have any further questions concerning this matter, please do not hesitate to contact the signatories below.

Respectfully,

Commerzbank AG
New York Branch

A handwritten signature in black ink, appearing to read "Deepa Keswani".

Deepa Keswani
Head of AML/Anti-Fraud/Sanctions Compliance

A handwritten signature in black ink, appearing to read "Vinay Jepal".

Vinay Jepal
Sanctions Compliance Officer

Encls.

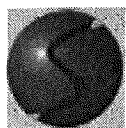
stratus intl payment

:LT Address	:COBAUS3XA
:transaction type	:202 COVER bank tfr favour 3rd bank
:input from	:COBADEFF
	COMMERZBANK AG FRANKFURT
	HEAD OFFICE
	32-36 NEUE MAINZERSTRASSE
	60261 FRANKFURT GERMANY
:Validation Flag	:COV}

{4: Text block:

:20 /transaction reference number	:FAAS109400150500
:21 /related reference	:FAAS109400150500
:32A/value date	:040411 USD 29,442,967.57
:52A/ordering institution - BIC	:COBADEFF
	COMMERZBANK AG
	FRANKFURT AM MAIN
:57A/account with inst - BIC	:CHASUS33
	JPMORGAN CHASE BANK, N.A.
	NEW YORK,NY
:58A/beneficiary inst - BIC	:SHHBCHZZ
	HYPOSWISS PRIVATBANK AG, ZURICH
	ZURICH
:50K/ordering customer	:/400887746602USD
	BT/ FIDEICOMISO / FONDO CHINO
	VENEZOLANO. AV GUICAIPURO. URB EL
	ROSAL. TORRE BANCO DEL TESORO.
	CARACAS - VENEZUELA.
:52A/ordering institution - BIC	:BDTEVECA
	BANCO DEL TESORO, C.A. BANCO
	UNIVERSAL
	CARACAS
:59 /beneficiary customer	:/CH7708530519663100203
	STRATUS INTERNATIONAL CONTRACTING
	J.S.
:70 /details of payment	:REF: DESEMBOLSO NRO. 386 FONDO
	CHINO VENEZOLANO. CODIGO NRO.
	00579.
:33B/amount	:USD 29,442,967.57}

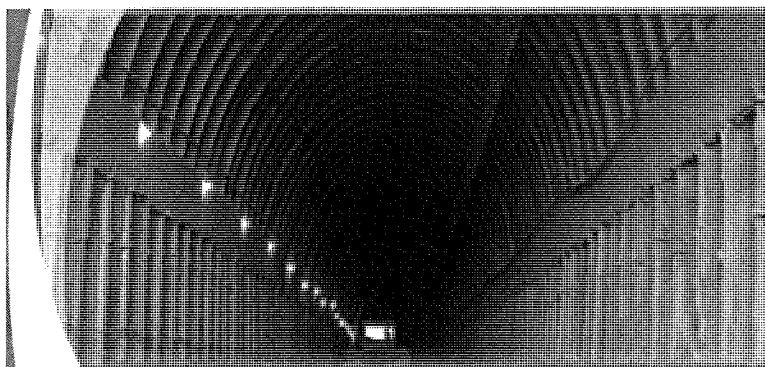
Entry : /SWIFT/ Date:110404 Time:02:44:17
Info:1111/001781



Stratus International
Contracting Company

فارسی | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of RIs 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



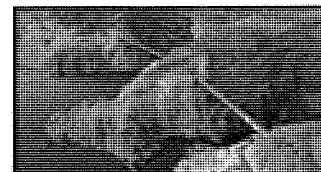
- STRATUS is an Engineering, Construction, Management and Contracting Company by specializing in the field of Building Construction, Road Works and Water Works.

STRATUS is Graded in three major categories: [Read more...](#)

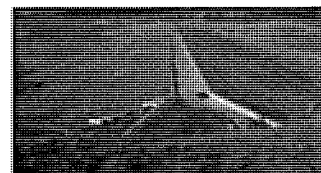
- STRATUS has succeeded to receive ISO 9001-2000 certificate for Quality Management System from MIC registered under UKAS, United Kingdom from 2004 which upgraded recently to ISO 9001-2008 in 2010 and intending to extend it by OHSAS 18001:2007. [Read more...](#)

- Our memberships:
 - Federation of Contractors of Islamic Countries (F.C.I.C.)
 - Pakistan Engineering Council
 - International Chamber of Commerce (I.C.C.)
 - Iran – UK Chamber of Commerce
 - Iran – Canada Chamber of Commerce [Read more...](#)

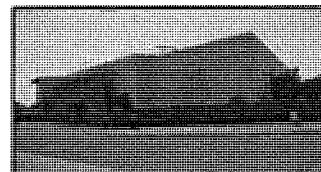
Road & Railway

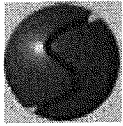


Dam



Building

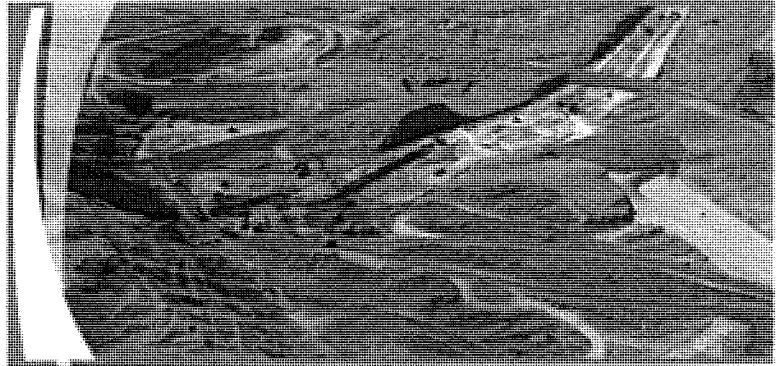




Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of RIs 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received "**Exemplary Exporters**" of the year 1999 from his excellency Mr. president.



Contact Us

STRATUS International Contracting Co.

Address: **No.35, Golestan St., Iran Zamin Ave., Shahrake Ghods, Tehran, Iran.**

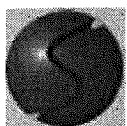
Postal Code: **1465865187**

Tell: **(98) 21 8837 3100-6**

Fax: **(98) 21 8808 2882**

E-mail: **stratus@stratusgc.com**

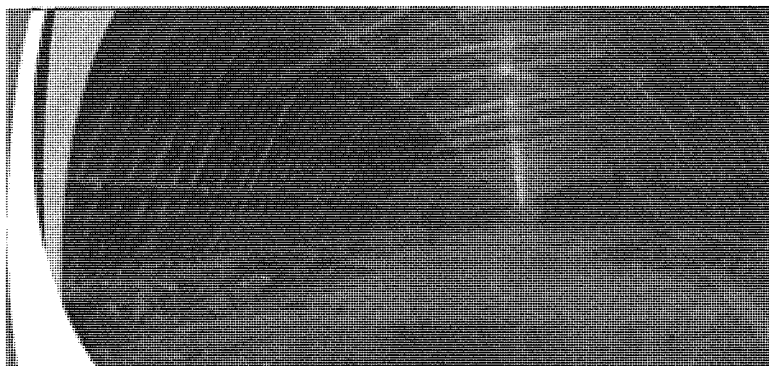
Copyright © 2010 Stratus Group Company. All rights reserved



Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of Rls 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



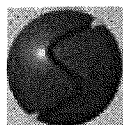
Branch Offices

Middle East
Iran
Iraq

CIS
Kazakhstan

South America
Venezuela

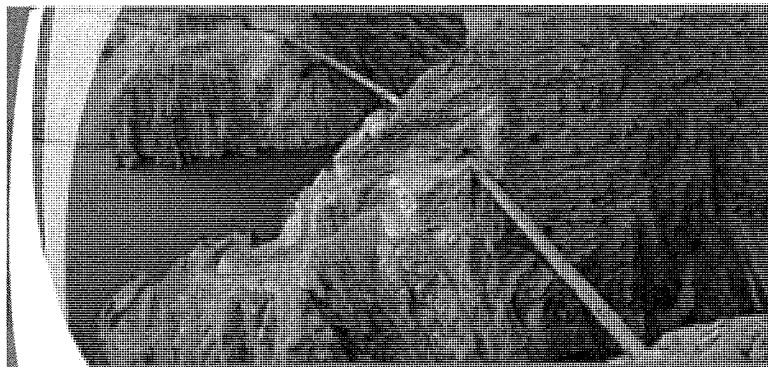
Copyright © 2010 Stratus Group Company. All rights reserved



Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

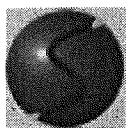
STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of RIs 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



Sister Companies List

-  1. Samaneh Stratus (INVESTMENT CO.)
-  2. Iran Construction Investment Co.
-  3. Eghtesad - Novin Bank
4. Pishgaman Bazar Novin (BROKERAGE CO.)
-  5. Novin Insurance Co.
-  6. Pars Shahr Co.
-  7. Global Petro Tech CO.
-  8. Keyhan Tabadol Co.
-  9. Pars Hanza Aluminium CO.
-  10. Azarbaijan Industry Development Co.
11. Eghtesad Novin Investment CO.
-  12. Samaneh Gostar Novin

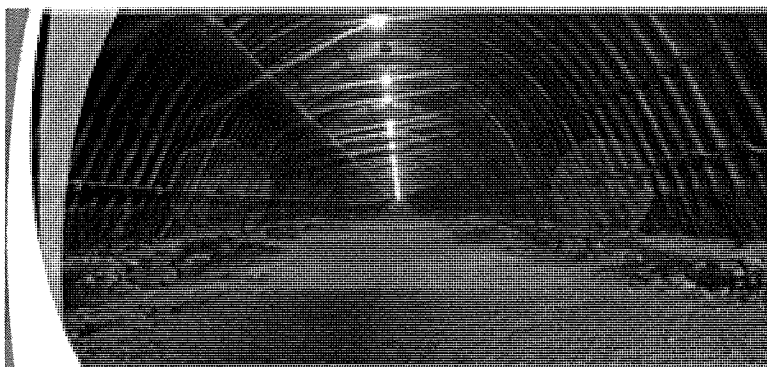
Copyright © 2010 Stratus Group Company. All rights reserved



Stratus International
Contracting Company

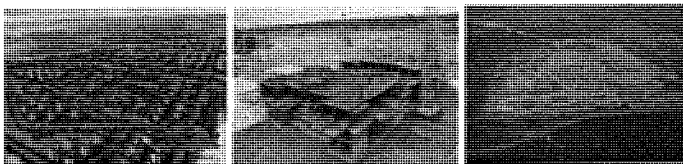
[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of RIs 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received "**Exemplary Exporters**" of the year 1999 from his excellency Mr. president.



7000 Units 'New Ojeda' Housing Development Project

Main Technical Features	Site Gross Area : 318 Hec. Concrete works : 520,000 m ³ Net Construction Area : 850.000 m ² Water & Sewage network : 150 Km Electrical network : 200 Km Communication network : 220 Km Gas network : 30 Km
Location	Ciudad Ojeda, Zulia State, Venezuela
Employer	Ducolsa 'Urban Development S.A'
Contract Duration	48 Months
Date of Award	September 2009
Status	[Under Construction]



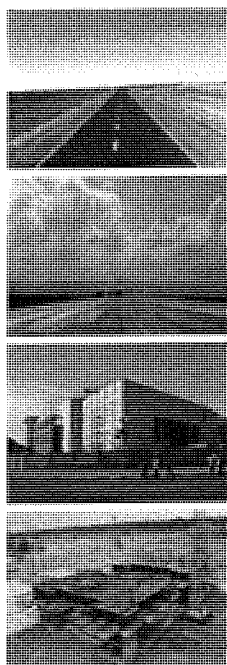
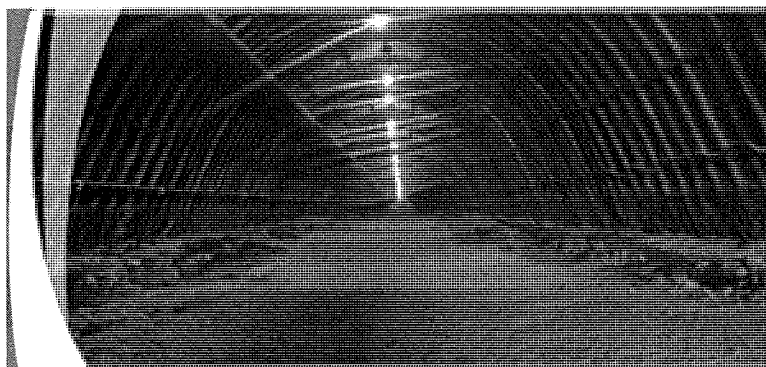
[\[Back to list\]](#)



Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of Rls 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



Dalbandin – Nokkundi Highway - Section III-B

[Details >>](#)

Socotra Airport

[Details >>](#)

Design & Construction of Parliament Building & Commercial Center in Djibouti City

[Details >>](#)

7000 Units "New Ojeda" Housing Development Project

[Details >>](#)

Copyright © 2010 Stratus Group Company. All rights reserved

T.C.
İSTANBUL
Ticaret Sicil Memurluğu

(KADIKÖY)
370857 - 2010

SİCİL TASDİKNAME Sİ

Ticaret Ünvanı	STRATUS INTERNATIONAL CONTRACTING İNŞAAT VE TAAHHÜT ANONİM ŞİRKETİ
Sicil No.	751671
Tescil Tarihi	22 / 10 / 2010
İşletme Merkezinin Adresi (Şubenin tescilinde şubenin Adresi ile beraber,merkezin adresi de yazılır.)	GARDENYA PLAZA 5 K.3 D.3 ATAŞEHİR
İşletmenin uğraştığı işler	Ana sözleşmesinde yazılı olan işler
İşletme sahibinin hüviyeti (Hükmi şahıslarda, hükmi şahsın mahiyeti)	Anonim
İşletme temsilcileri	38824643592 TC.No.lu CELAL TATLICIBAŞI
Tasdiknamenin düzenlenme Tarih ve Sayısı	22 EKİM 2010 - 39185

RECAİ SÖKMEN
İSTANBUL TİCARET SİCİLİ
MEMURU YARDIMCISI

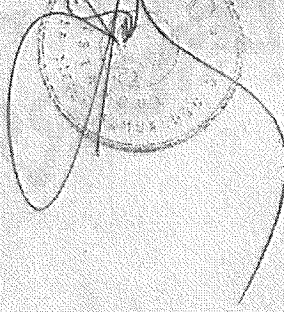


EXHIBIT 26

Kim, Jane (USANYS) 4

From: Milione, Shawn (USANYS) [Contractor]
Sent: Saturday, March 7, 2020 10:52 AM
To: Lake, Stephanie (USANYS)
Cc: Krouse, Michael (USANYS); Kim, Jane (USANYS) 4; Lynch, Garrett (USANYS) [Contractor]
Subject: Re: GX 411

Hey, I'm at the gym right now but can do it as soon as I get back to my apartment. I should be done in about an hour. Is that okay?

Sent from my iPhone

> On Mar 7, 2020, at 10:48 AM, Lake, Stephanie (USANYS) <SLake@usa.doj.gov> wrote:
>
> Hey Shawn,
>
> Can you let me know when you think you'll have a chance to mark this GX 411? If you won't be in for a while and can tell me how to do it, I'm happy to do it myself!
>
> Thanks!
>
> Stephanie Lake
> Assistant United States Attorney
> Southern District of New York
> One Saint Andrew's Plaza
> New York, NY 10007
> Tel: (212) 637-1066
>
> <Commerz OFAC disclosure.pdf>

EXHIBIT 27

Kim, Jane (USANYS) 4

From: Lake, Stephanie (USANYS)
Sent: Saturday, March 7, 2020 4:04 PM
To: Weingarten, Reid; Heberlig, Brian; Silverman, Nicholas
Cc: Krouse, Michael (USANYS); Kim, Jane (USANYS) 4; Lynch, Garrett (USANYS) [Contractor]; Milione, Shawn (USANYS) [Contractor]
Subject: U.S. v. Sadr
Attachments: GX 2284D.pdf; 3508-008.pdf; GX 411.pdf; GX 456.pdf; GX 495A 2280 Statements.pdf; GX 495B 9288 Statements.pdf; GX 704_Redacted.pdf; GX 705A.pdf; GX 705B.pdf; GX 2304A (rev'd 2020.3.7).pdf; 3504-10.pdf; 3505-06.pdf; 3513-02.pdf; 3513-03.pdf

Counsel,

Mr. Dubowitz is still very ill. As a result, we do not intend to call him as a witness in our case-in-chief. It's possible that, depending on the defense case, we will call him as a rebuttal witness.

In addition, we've attached the following documents:

- Updated GX 2284D – there were formatting problems with our version. We think the attached corrects them.
- 3508-08 – 3500 from today
- GX 411 – we intend to offer this on Monday. Let us know if you will stipulate to authenticity.
- GX 456 – we intend to offer this on Monday. Let us know if you will stipulate to authenticity.
- GX 495A & B – we intend to offer these on Monday (likely in redacted form), although think a stipulation that the defendant had bank accounts at HSBC from January 2010 through October 2013 might be simpler. Let us know how you prefer to proceed.
- GX 704 – this is the modified version of the travel chart. Please confirm whether you have any remaining concerns.
- GX 705A & B – these are summary charts reflecting the information in GX 2090A. Please confirm whether you have any objections.
- Updated GX 2304A – we enlarged some of the cells, as the formatting of the PDFd excel file was cutting off some of the data. The content is the same.
- 3504-10 – Peri 3500, which was provided in hard copy yesterday morning.
- 3505-06 – Blair 3500, which was provided in hard copy yesterday morning.
- 3513-02 – Paralegal 3500 for summary chart (you may already have this)
- 3513-03 – Paralegal 3500 for summary chart (you may already have this)

We are still working on one additional summary chart, which we expect to provide later today.

Stephanie Lake
Assistant United States Attorney
Southern District of New York
One Saint Andrew's Plaza
New York, NY 10007
Tel: (212) 637-1066

EXHIBIT 27-1

HYPOSWISS

PRIVATE BANK

Hyposwiss Private Bank Ltd.
 Stauffacherstrasse 41
 CH-8004 Zurich
 Phone +41 (0)44 214 31 11
 Fax +41 (0)44 211 52 23
 www.hyposwiss.ch
 BIC SHHBCHZZ

Your contact person:
 Marchetti Luca
 Direct +41 (0) 44 214 32 50
 luca.marchetti@hyposwiss.ch

Clarity Trade & Finance SA

Current account USD 5182061.203
 IBAN CH80 0853 0518 2061 0020 3

Clarity Trade & Finance SA
 Wächlenstrasse 5
 8832 Wollerau

Zurich, June 26, 2012

USD Account statement 01.01.2012 - 25.06.2012

Date	Text	Debit	Credit	Value date	Balance
01.01.	Balance carried forward				3,804,704.63
04.01.	Credit advice / Ref. no. 335408743 1/PDVSA PETROLEOSA 2/AV LIBERTADOR ED PDVSA T EST PISO 2/TESOURARIA APARTADO 169 A LA CAMP 3/VE/CARACAS 1060 VENEZUELA 1501958361 ZP 8021 CTY ZURICH DDA 000000000 11835873 CHPU 059242 DIR BAHNHO FSTRASSESCHUETZENGASSE 4 DIR1 POSTF		6,704,753.09	30.12.11	10,509,457.72
05.01.	Debit advice / Ref. no. 335575588 Stratus Global Investments Ltd	1,006,414.25		05.01.12	9,503,043.47
09.01.	Debit advice / Ref. no. 336096647 Stratus Global Investments Ltd	228,747.95		09.01.12	9,274,295.52
16.01.	Debit advice / Ref. no. 337121029 Clarity Trade & Finance SA	657,456.42		16.01.12	8,616,839.10
18.01.	Debit advice / Ref. no. 337608857 Clarity Trade & Finance SA	3,850,200.00		18.01.12	4,766,639.10
24.01.	Debit advice / Ref. no. 338662584 A+R CAPITAL PARTNERS LLC SOLE OWNER: ALI SADR 7117 NATELLI WOODS LANE BETHESDA MD 20817 USA Cost: USD 20.00	1,000,020.00		24.01.12	3,766,619.10
01.02.	Debit advice / Ref. no. 340660144 FIDELITY NATIONAL TITLE COMPANY 8050 N.PALM AVENUE, SUITE 110 FRESNO, CA 93711 Cost: USD 20.00	2,226,020.00		01.02.12	1,540,599.10
02.02.	Debit advice / Ref. no. 340865894 Stratus Global Investments Ltd	312,252.80		02.02.12	1,228,346.30
03.02.	Debit advice / Ref. no. 341091335 Stratus Global Investments Ltd	45,020.00		03.02.12	1,183,326.30

**GOVERNMENT
EXHIBIT
2284D
18 Cr. 224 (AJN)**

HYPOSWISS

PRIVATE BANK

Clarity Trade & Finance SA

Current account USD 5182061.203

IBAN CH80 0853 0518 2061 0020 3

Date	Text	Debit	Credit	Value date	Balance
06.02.	Debit advice / Ref. no. 341397968 Stratus Global Investments Ltd	45,020.00		06.02.12	1,138,306.30
07.02.	Debit Forex Spot USD/CHF 0.904352 on February 7, 2012 CHF 46,377.45 Exchange rate: 1.105764 (CHF/USD)	51,282.52		09.02.12	1,087,023.78
07.02.	Debit advice / Ref. no. 341555765 Stratus Global Investments Ltd	25,020.00		07.02.12	1,062,003.78
09.02.	Debit Forex Spot USD/CHF 0.900946 on February 9, 2012 CHF 7,376.75 Exchange rate: 1.109945 (CHF/USD)	8,187.78		13.02.12	1,053,816.00
13.02.	Debit advice / Ref. no. 342310384 Stratus Global Investments Ltd	45,020.00		13.02.12	1,008,796.00
28.02.	Debit Forex Spot EUR/USD 1.345500 on February 28, 2012 EUR 250,000.00 Exchange rate: 1.3455 (EUR/USD)	336,375.00		28.02.12	672,421.00
28.02.	Debit advice / Ref. no. 344773308 Stratus Global Investments Ltd	142,000.00		28.02.12	530,421.00
01.03.	Debit advice / Ref. no. 345434097 Stratus Global Investments Ltd	47,957.14		01.03.12	482,463.86
05.03.	Debit advice / Ref. no. 346025962 Stratus Global Investments Ltd	90,471.33		05.03.12	391,992.53
06.03.	Incoming Payment / Ref. no. 346230844 A R CAPITAL PARTNERS LLC 7117 NATELLI WOODS LN BETHESDA MD 20817-3927 BETHESDA Information: /RFB/BI11176720650002		999,980.00	06.03.12	1,391,972.53
07.03.	Debit advice / Ref. no. 346385767 Stratus Global Investments Ltd	101,431.00		07.03.12	1,290,541.53
07.03.	Debit advice / Ref. no. 346408745 Stratus Global Investments Ltd	520.00		07.03.12	1,290,021.53
07.03.	Debit Forex Spot USD/CHF 0.906624 on March 7, 2012 CHF 285.00 Exchange rate: 1.102993 (CHF/USD)	314.35		09.03.12	1,289,707.18
21.03.	Debit Forex Spot USD/CHF 0.896699 on March 21, 2012 CHF 27,379.40 Exchange rate: 1.115201 (CHF/USD)	30,533.55		23.03.12	1,259,173.63
23.03.	Debit advice / Ref. no. 348778399 Yasemin Cetinel Valikonagi Cad. Prof. Dr. Muefide Kueley Sok. Camlibel Apt 51/3 Nisantasi / Istanbul TURKIYE Amount: TRY 2,500.00 Cost: TRY 40.00 Exchange rate: 0.565271 (TRY/USD)	1,435.79		23.03.12	1,257,737.84

HYPOSWISS

PRIVATE BANK

Clarity Trade & Finance SA

Current account USD 5182061.203

IBAN CH80 0853 0518 2061 0020 3

Date	Text	Debit	Credit	Value date	Balance
02.04.	Debit Forex Spot USD/CHF 0.893589 on April 2, 2012 CHF 105.31 Exchange rate: 1.119083 (CHF/USD)	117.85		04.04.12	1,257,619.99
02.04.	Debit Forex Spot USD/CHF 0.893441 on April 2, 2012 CHF 8.47 Exchange rate: 1.119269 (CHF/USD)	9.48		02.04.12	1,257,610.51
11.04.	Debit advice / Ref. no. 352398458 Stratus Global Investments Ltd	39,621.00		11.04.12	1,217,989.51
11.04.	Debit advice / Ref. no. 352410809 Malibu Escrow Corp. 22241 Pacific Coast Highway Malibu, CA 90265 Cost: USD 20.00	920,020.00		11.04.12	297,969.51
12.04.	Debit Forex Spot USD/CHF 0.903414 on April 12, 2012 CHF 6,463.55 Exchange rate: 1.106912 (CHF/USD)	7,154.58		12.04.12	290,814.93
13.04.	Credit advice / Ref. no. 352735783 Clarity Trade & Finance SA		209,205.07	13.04.12	500,020.00
13.04.	Debit advice / Ref. no. 352760348 Stratus Global Investments Ltd	500,020.00		13.04.12	0.00
19.04.	Debit advice / Ref. no. 353758782 YASEMIN CETINEL Valikonagi Cad.Prof.Dr. Muefide Kueley Sok., Camlibel Apt 51/3 Nisantasi/Istanbul/Turkuye Amount: TRY 2,500.00 Cost: TRY 40.00 Exchange rate: 0.567372 (TRY/USD)	1,441.12		19.04.12	-1,441.12
20.04.	Credit advice / Ref. no. 353845677 Clarity Trade & Finance SA		1,441.12	19.04.12	0.00
27.04.	Credit advice / Ref. no. 355619871 Clarity Trade & Finance SA		2,000,000.00	27.04.12	2,000,000.00
30.04.	Debit advice / Ref. no. 356117327 Sapene LLC 1134 Alta Loma rd 303 W. Hollywood CA 90069 Cost: USD 20.00	1,089,020.00		30.04.12	910,980.00
07.05.	Debit advice / Ref. no. 357428326 Stratus Global Investments Ltd	500,000.00		07.05.12	410,980.00
07.05.	Debit Forex Spot USD/CHF 0.912450 on May 7, 2012 CHF 13,675.22 Exchange rate: 1.095950 (CHF/USD)	14,987.36		07.05.12	395,992.64
07.05.	Debit Forex Spot EUR/USD 1.323153 on May 7, 2012 EUR 1,760.00 Exchange rate: 1.323153 (EUR/USD)	2,328.75		07.05.12	393,663.89
09.05.	Debit Forex Spot USD/CHF 0.915709 on May 9, 2012 CHF 3,941.55 Exchange rate: 1.092050 (CHF/USD)	4,304.37		09.05.12	389,359.52

ban to P. Sadr
own transaction ✓

HYPOSWISS

PRIVATE BANK

Clarity Trade & Finance SA

Current account USD 5182061.203

IBAN CH80 0853 0518 2061 0020 3

<i>Date</i>	<i>Text</i>	<i>Debit</i>	<i>Credit</i>	<i>Value date</i>	<i>Balance</i>
10.05.	Debit Forex Spot EUR/USD 1.310825 on May 10, 2012 EUR 1,107.00 Exchange rate: 1.310825 (EUR/USD)	1,451.08		10.05.12	387,908.44
11.05.	Debit advice / Ref. no. 358142982 Damon Chung Cost: USD 20.00	6,020.00		11.05.12	381,888.44
21.05.	Debit advice / Ref. no. 359196048 A + R Capital Partners, LLC 7117 Natelli Woods Lane Bethesda, MD 20817 USA Cost: USD 20.00	64,320.00		21.05.12	317,568.44
01.06.	Debit Forex Spot EUR/USD 1.239065 on June 1, 2012 EUR 35,000.00 Exchange rate: 1.239065 (EUR/USD)	43,367.28		01.06.12	274,201.16
08.06.	Debit Forex Spot USD/CHF 0.958500 on June 8, 2012 CHF 26,929.05 Exchange rate: 1.043297 (CHF/USD)	28,094.99		08.06.12	246,106.17
12.06.	Debit Forex Spot USD/CHF 0.949333 on June 12, 2012 CHF 5,952.35 Exchange rate: 1.053371 (CHF/USD)	6,270.03		12.06.12	239,836.14
18.06.	Debit Forex Spot USD/CHF 0.941828 on June 18, 2012 CHF 196.00 Exchange rate: 1.061765 (CHF/USD)	208.11		18.06.12	239,628.03
Volume of transactions		13,480,455.88	9,915,379.28		
25.06.	Balance				239,628.03

Please check this statement carefully. Should you find any discrepancies, please contact us within 30 days.

EXHIBIT 27-2

Conte

Fazio, DePresco, Lata 3/7/10

August 2011 - December 6, 2011

Contract - \$170,000

Sept. 7 - \$34k USD deposit

End month, closed \$52,700 wire -> Balance \$83,300

Person who bought unit ^{was} issued ~~for~~ a mortgage in Bolivers

Bank advanced Boliver loan to her for mortgage value

needed in USD. Buyer's father arranged transfer through schemes of

\$23,000 stayed in Bolivers

\$60,000 was balance of money owed

Prep

cross

Logistics

EXHIBIT 27-3



NEW YORK BRANCH

Department of the Treasury
Office of Foreign Assets Control
1500 Pennsylvania Avenue NW
Washington DC 20220

Vinay Jepak
2 World Financial Center, New York, NY 10281-1050
Telephone (212) 266-7200
Fax (212) 266-7235
vinay.jepak@commerzbank.com

June 16, 2011

Re: Information Sharing – Stratus International Contracting Company

Dear Sir/Madam:

Commerzbank AG, New York Branch (CBNY) would like to share the following information with OFAC. On April 20, 2011 CBNY's AML transaction monitoring system generated an alert, which involved a transaction for USD 29,442,967.57 value April 4, 2011.

The transaction was originated by Banco Del Tesoro, CA Banco Universal Caracas for its client BT / Fideicomiso / Fondo Chino Venezolano in Caracas, Venezuela. The beneficiary of the payment was Stratus International Contracting Company ("Stratus"), a client of Hyposwiss Privatbank AG, Zurich.

As per standard procedure, CBNY initiated a request for information to the remitting bank Banco Del Tesoro, CA Banco Universal Caracas, Venezuela to obtain details on both entities and their relationship. In the interim, CBNY conducted further due diligence and noted the following regarding Stratus from its website:

- Stratus was founded in 1978 in Tehran, Iran
- Stratus International specializes in providing contracting services to infrastructure projects such as roads, railways, dams, tunnels, airports and buildings.
- Stratus is presently working on a 7000 Apartment Unit "New Ojeda" Housing Development Project in Venezuela

On May 12, 2011, CBNY received a response from the bank in Caracas indicating the following:

- Stratus's physical address is Gardenya Plaza 5, K:3 D:3 (Floor 3, Suite3) 34758 Atasehir, Istanbul, Turkey
- Stratus is registered in Istanbul, Turkey (copy of the registration attached)
- Stratus provides construction services in Turkey, Dubai and Venezuela
- The purpose of the payment is for the construction of a 7000 apartment unit project "Proyecto Urbanismo Nueva Ciudad Fabricio Ojeda, in Ciudad Ojeda, Estado Zulia, Venezuela (same address as listed on Stratus' website)

Although Stratus is not listed as an SDN, and the payment does not indicate any direct involvement of Iran or with Iran, due to conflicting information between the website and the response forwarded by the bank in Caracas, CBNY believes it appropriate to share this information with OFAC since Stratus may be an Iranian Company.

Chairman of the Supervisory Board: Klaus-Peter Müller
Board of Managing Directors: Martin Blessing (Chairman),
Frank Annuscheit, Markus Beumer, Achim Kassow, Jochen Klösges,
Michael Reuther, Stefan Schmittmann, Ulrich Sieber, Eric Strutz, Martin Zielke

Commerzbank Aktiengesellschaft, Frankfurt am Main
Registered Office: Frankfurt am Main Reg.No. 32000
VAT No. DE 114 103 514



NEW YORK BRANCH

Re: Information Sharing – Stratus International Contracting Company– Page 2

We have added Stratus into our sanctions filter to monitor any future payments. Please note that apart from this transaction, there have not been any other payments involving Stratus processed by CBNY to date.

The purpose of this letter is to report the good faith efforts of Commerzbank AG, New York Branch in complying with applicable OFAC requirements and voluntarily informing OFAC of any information received during its investigation into possible sanctions-related entities.

Should you have any further questions concerning this matter, please do not hesitate to contact the signatories below.

Respectfully,

Commerzbank AG
New York Branch

A handwritten signature in dark ink, appearing to read "Deepa Keswani".

Deepa Keswani
Head of AML/Anti-Fraud/Sanctions Compliance

A handwritten signature in dark ink, appearing to read "Vinay Jepal".

Vinay Jepal
Sanctions Compliance Officer

Encls.

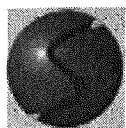
stratus intl payment

:LT Address	:COBAUS3XA
:transaction type	:202 COVER bank tfr favour 3rd bank
:input from	:COBADEFF
	COMMERZBANK AG FRANKFURT
	HEAD OFFICE
	32-36 NEUE MAINZERSTRASSE
	60261 FRANKFURT GERMANY
:Validation Flag	:COV}

{4: Text block:

:20 /transaction reference number	:FAAS109400150500
:21 /related reference	:FAAS109400150500
:32A/value date	:040411 USD 29,442,967.57
:52A/ordering institution - BIC	:COBADEFF
	COMMERZBANK AG
	FRANKFURT AM MAIN
:57A/account with inst - BIC	:CHASUS33
	JPMORGAN CHASE BANK, N.A.
	NEW YORK,NY
:58A/beneficiary inst - BIC	:SHHBCHZZ
	HYPOSWISS PRIVATBANK AG, ZURICH
	ZURICH
:50K/ordering customer	:/400887746602USD
	BT/ FIDEICOMISO / FONDO CHINO
	VENEZOLANO. AV GUICAIPURO. URB EL
	ROSAL. TORRE BANCO DEL TESORO.
	CARACAS - VENEZUELA.
:52A/ordering institution - BIC	:BDTEVECA
	BANCO DEL TESORO, C.A. BANCO
	UNIVERSAL
	CARACAS
:59 /beneficiary customer	:/CH7708530519663100203
	STRATUS INTERNATIONAL CONTRACTING
	J.S.
:70 /details of payment	:REF: DESEMBOLSO NRO. 386 FONDO
	CHINO VENEZOLANO. CODIGO NRO.
	00579.
:33B/amount	:USD 29,442,967.57}

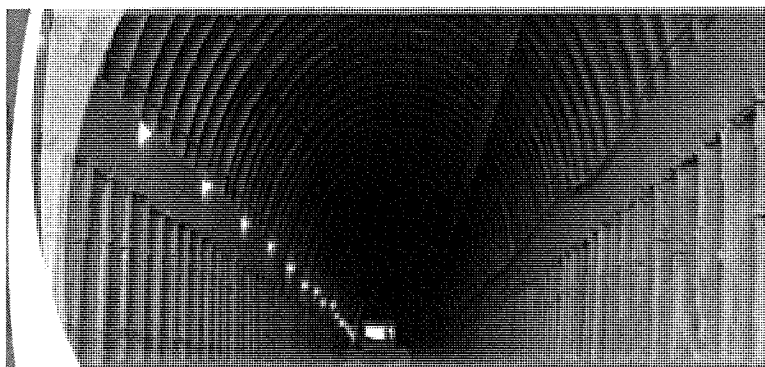
Entry : /SWIFT/ Date:110404 Time:02:44:17
Info:1111/001781



Stratus International
Contracting Company

فارسی | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of RIs 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



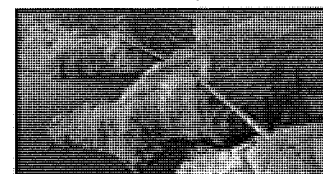
- STRATUS is an Engineering, Construction, Management and Contracting Company by specializing in the field of Building Construction, Road Works and Water Works.

STRATUS is Graded in three major categories: [Read more...](#)

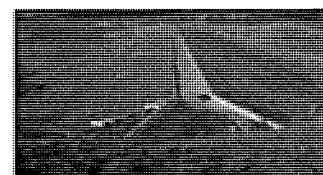
- STRATUS has succeeded to receive ISO 9001-2000 certificate for Quality Management System from MIC registered under UKAS, United Kingdom from 2004 which upgraded recently to ISO 9001-2008 in 2010 and intending to extend it by OHSAS 18001:2007. [Read more...](#)

- Our memberships:
 - Federation of Contractors of Islamic Countries (F.C.I.C.)
 - Pakistan Engineering Council
 - International Chamber of Commerce (I.C.C.)
 - Iran – UK Chamber of Commerce
 - Iran – Canada Chamber of Commerce [Read more...](#)

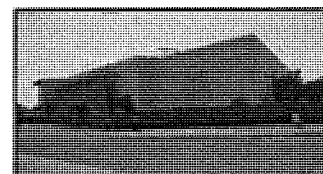
Road & Railway

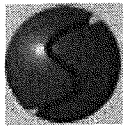


Dam



Building

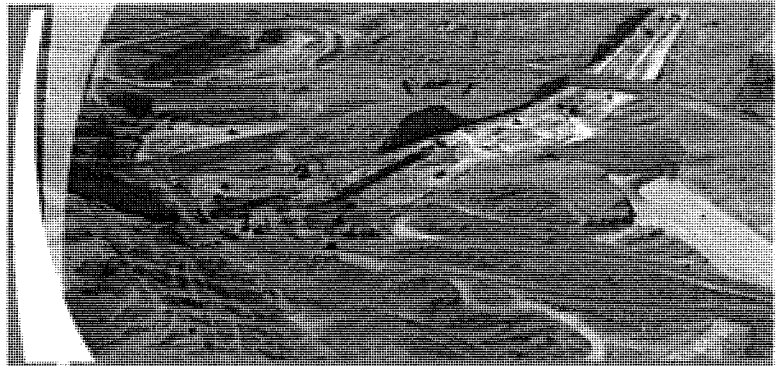




Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of RIs 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received "**Exemplary Exporters**" of the year 1999 from his excellency Mr. president.



Contact Us

STRATUS International Contracting Co.

Address: **No.35, Golestan St., Iran Zamin Ave., Shahrake Ghods, Tehran, Iran.**

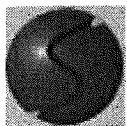
Postal Code: **1465865187**

Tell: **(98) 21 8837 3100-6**

Fax: **(98) 21 8808 2882**

E-mail: **stratus@stratusgc.com**

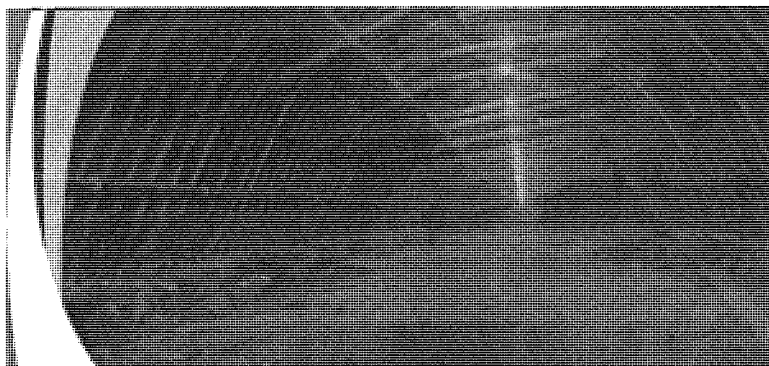
Copyright © 2010 Stratus Group Company. All rights reserved



Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of Rls 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



Branch Offices

Middle East
Iran
Iraq

CIS
Kazakhstan

South America
Venezuela

Copyright © 2010 Stratus Group Company. All rights reserved



Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of Rls 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



Sister Companies List



1. Samaneh Stratus (INVESTMENT CO.)



2. Iran Construction Investment Co.



3. Eghtesad - Novin Bank

4. Pishgaman Bazar Novin (BROKERAGE CO.)



5. Novin Insurance Co.



6. Pars Shahr Co.



7. Global Petro Tech CO.



8. Keyhan Tabadol Co.



9. Pars Hanza Aluminium CO.



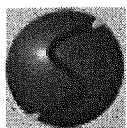
10. Azarbaijan Industry Development Co.

11. Eghtesad Novin Investment CO.



12. Samaneh Gostar Novin

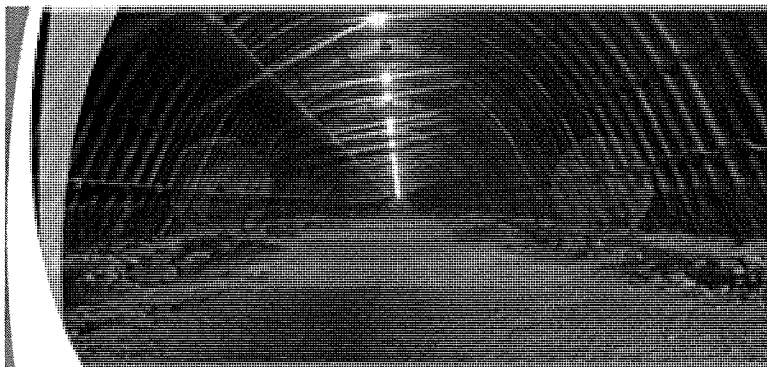
Copyright © 2010 Stratus Group Company. All rights reserved



Stratus International
Contracting Company

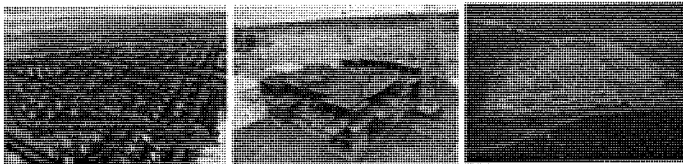
[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of RIs 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received "**Exemplary Exporters**" of the year 1999 from his excellency Mr. president.



7000 Units 'New Ojeda' Housing Development Project

Main Technical Features	Site Gross Area : 318 Hec. Concrete works : 520,000 m ³ Net Construction Area : 850.000 m ² Water & Sewage network : 150 Km Electrical network : 200 Km Communication network : 220 Km Gas network : 30 Km
Location	Ciudad Ojeda, Zulia State, Venezuela
Employer	Ducolsa 'Urban Development S.A'
Contract Duration	48 Months
Date of Award	September 2009
Status	[Under Construction]



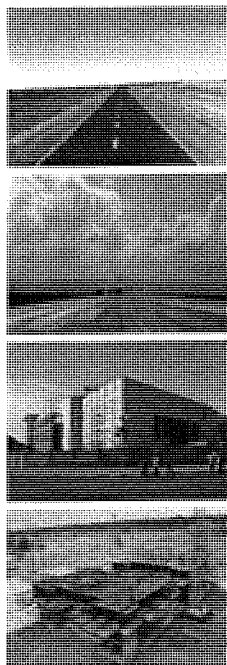
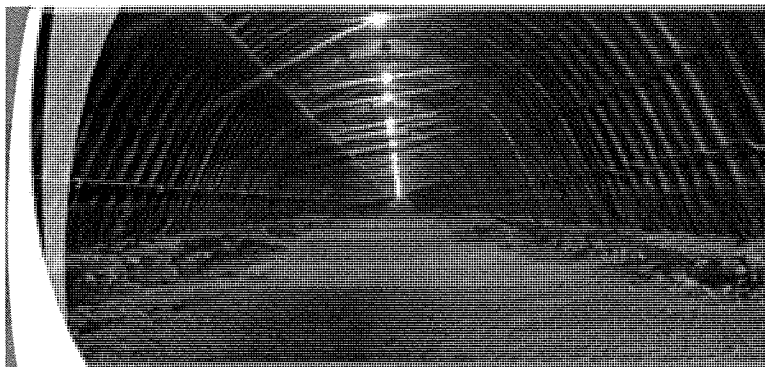
[\[Back to list\]](#)



Stratus International
Contracting Company

[فارسی](#) | [Staff Login](#) | [Site Map](#) | [Hon](#)

STRATUS International Contracting Company has been founded in 1978 in Tehran, Iran, with registered paid up share capital of Rls 100 billions. STRATUS provides contracting services to infrastructure projects such as Roads, Railways, Dams, Tunnels, Airports and Buildings. Since 1994, STRATUS has been the first pioneered company in exporting Engineering and Technical Services in Iran and received **"Exemplary Exporters"** of the year 1999 from his excellency Mr. president.



Dalbandin – Nokkundi Highway - Section III-B

[Details >>](#)

Socotra Airport

[Details >>](#)

Design & Construction of Parliament Building & Commercial Center in Djibouti City

[Details >>](#)

7000 Units "New Ojeda" Housing Development Project

[Details >>](#)

T.C.
İSTANBUL
Ticaret Sicil Memurluğu

(KADIKÖY)
370857 - 2010

SİCİL TASDİKNAMESİ

Ticaret Ünvanı	STRATUS INTERNATIONAL CONTRACTING İNŞAAT VE TAAHHÜT ANONİM ŞİRKETİ
Sicil No.	751671
Tescil Tarihi	22 / 10 / 2010
İşletme Merkezinin Adresi (Şubenin tescilinde şubenin Adresi ile beraber,merkezin adresi de yazılır.)	GARDENYA PLAZA 5 K.3 D.3 ATAŞEHİR
İşletmenin uğraştığı işler	Ana sözleşmesinde yazılı olan işler
İşletme sahibinin hüviyeti (Hükmi şahıslarda, hükmi şahsın mahiyeti)	Anonim
İşletme temsilcileri	38824643592 TC.No.lu CELAL TATLICIBAŞI
Tasdiknamenin düzenlenme Tarih ve Sayısı	22 EKİM 2010 - 39185

RECAİ SÖKMEN
İSTANBUL TİCARET SİCİLİ
MEMURU YARDIMCISI

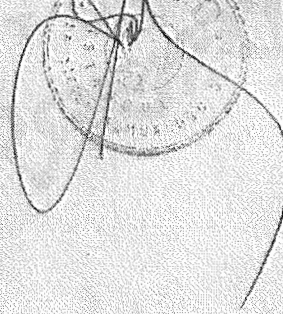


EXHIBIT 27-4

Business Account Application

**WELLS
FARGO**

Bank Name: Wells Fargo Bank, N.A.		Store Name: MALIBU	
Banker Name: MAKSIM KOLOMEYER		Officer/Portfolio Number: CG678	Date: 01/26/2012
Banker Phone: 310/317-1740	Store Number: 04649	Banker AID: 0001902	Banker MAC: E2351-011

To help the government fight the funding of terrorism and money laundering activities, U.S. Federal law requires financial institutions to obtain, verify, and record information that identifies each person (individuals and businesses) who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

New Account Information

☒ New Deposit Account(s) Only ☐ New Deposit Account(s) and Business Credit Card

Account Product Name Expanded Business Services Package				
COID: 114	Product: DDA	Account Number: 2807883273	Opening Deposit: \$1,000.00	Type of Funds: CKS

New Account Kit: Printed

Authorized Signers

Business Name: PISTACHE LLC	Other Related Customer Name:
Authorized Signer Name(s): SADEGH AMINIAN SEYED MOHSEN TORABI	PEGAN SADRHASHEMINEJAD



BBG2307 (11-11 SVP)

2W02-000469155618-01

**GOVERNMENT
EXHIBIT
456**

18 Cr. 224 (AJN)

Business Account Application

Checking/Savings Statement Mailing Information

Name(s) and Information Listed on Statement: PISTACHE LLC	Statement Mailing Address: 429 18TH ST	
	Address Line 2:	
	City: SANTA MONICA	State: CA
	ZIP/Postal Code: 90402-2429	Country: US

Business Information

Business Name: PISTACHE LLC		Street Address: 429 18TH ST	
Taxpayer Identification Number (TIN): 45-4306973		Address Line 2:	
TIN Type: EIN		Address Line 3:	
Business Type: Limited Liability Company			
Business Sub-Type:	Non-Profit: No	City: SANTA MONICA	State: CA
Date Originally Established: 01/17/2012	Current Ownership Since:	ZIP/Postal Code: 90402-2429	Country: US
Number of Employees: 5			
Annual Gross Sales: \$1,000,000.00	Year Sales Reported: 01/01/2012	Fiscal Year End:	Business Phone: (310) 383-5459
			Fax:
Primary Financial Institution:	Number of Locations: 1	Cellular Phone:	Pager:
Sales Market: LOCAL		e-Mail Address:	
Primary State 1:	Primary State 2:	Primary State 3:	Website:
Primary Country 1:	Primary Country 2:	Primary Country 3:	
Industry: Agriculture, Forestry, Fishing and Hunting			
Description of Business: Pistachio Farm			
Major Suppliers/Customers:			

Bank Use Only

Name/Entity Verification: Articles of Organization		Address Verification:		BACC Reference Number: 612BAC5128026
Document Filing Number/Description: 201201810090	Filing Country: US	Filing State: CA	Filing Date: 01/17/2012	Expiration Date:
Country of Registration: US	State of Registration: CA	International Transactions:		Check Reporting: NO RECORD
Internet Gambling Business No				



Business Account Application

Owner/Key Individual 1 Information

Customer Name: SADEGH AMINIAN		Residence Address: 429 18TH ST	
Position/Title: OWNER	Date of Birth: 12/09/1958	Address Line 2:	
Taxpayer Identification Number (TIN): 563-59-0567	TIN Type: SSN	Address Line 3:	
Primary ID Type: DLIC	Primary ID Description: C0033250	City: SANTA MONICA	State: CA
Primary ID St/Ctry/Prov: CA	Primary ID Issue Date: 12/01/2009	Primary ID Expiration Date: 12/09/2014	ZIP/Postal Code: 90402-2429
Secondary ID Type: OTHR DC	Secondary ID Description: WF VISA	Check Reporting: NO RECORD	
Secondary ID State/Country:	Secondary ID Issue Date:	Secondary ID Expiration Date: 07/01/2012	
Country of Citizenship: US			

Owner/Key Individual 2 Information

Customer Name: PEGAH SADRHASHEMINEJAD		Residence Address: 1134 ALTA LOMA RD APT 303	
Position/Title: PARTNER	Date of Birth: 02/10/1979	Address Line 2:	
Taxpayer Identification Number (TIN): 141-06-3068	TIN Type: SSN	Address Line 3:	
Primary ID Type: DLIC	Primary ID Description: S-362-680-007-108	City: WEST HOLLYWOOD	State: CA
Primary ID St/Ctry/Prov: MD	Primary ID Issue Date: 10/07/2010	Primary ID Expiration Date: 02/10/2016	ZIP/Postal Code: 90069-2433
Secondary ID Type: OTHR CC	Secondary ID Description: HSBC CC	Check Reporting: NO RECORD	
Secondary ID State/Country:	Secondary ID Issue Date: 01/01/2010	Secondary ID Expiration Date: 01/01/2013	
Country of Citizenship: IR	Permanently Resides in US: YES		



Owner/Key Individual 3 Information

Customer Name: SEYED MOHSEN TORABI			Residence Address: 3131 MICHELSON DR UNIT 1601	
Position/Title: OWNER		Date of Birth: 09/20/1967		Address Line 2:
Taxpayer Identification Number (TIN): 624-85-8966		TIN Type: SSN		Address Line 3:
Primary ID Type: DLIC	Primary ID Description: F2662158		City: IRVINE	State: CA
Primary ID St/Ctry/Prov: CA	Primary ID Issue Date: 03/16/2011	Primary ID Expiration Date: 03/10/2012	ZIP/Postal Code: 92612-5666	Country: US
Secondary ID Type: ALID PR	Secondary ID Description: 061-381-569		Check Reporting: NO RECORD	
Secondary ID State/Country:	Secondary ID Issue Date: 03/10/2011	Secondary ID Expiration Date: 03/10/2013		
Country of Citizenship: IR	Permanently Resides in US: YES			

Certificate of Authority

Each person who signs the "Certified/Agreed To" section of this Application certifies that:

- A. The Customer's use of any Bank deposit account, product or service will confirm the Customer's receipt of, and agreement to be bound by, the Bank's applicable fee and information schedule and account agreement that includes the Arbitration Agreement under which any dispute between the Customer and the Bank relating to the Customer's use of any Bank deposit account, product or service will be decided in an arbitration proceeding before a neutral arbitrator as described in the Arbitration Agreement and not by a jury or court trial.**
- B. Each person who signs the "Certified/Agreed To" section of this Application or whose name, any applicable title and specimen signature appear in the "Authorized Signers - Signature Capture" section of this Application is authorized on such terms as the Bank may require to:**
- (1) Enter into, modify, terminate and otherwise in any manner act with respect to accounts at the Bank and agreements with the Bank or its affiliates for accounts and/or services offered by the Bank or its affiliates (other than letters of credit or loan agreements);
 - (2) Authorize (by signing or otherwise) the payment of Items from the Customer's account(s) listed on this Business Account Application (including without limitation any Item payable to (a) the individual order of the person who authorized the Item or (b) the Bank or any other person for the benefit of the person who authorized the Item) and the endorsement of Deposited Items for deposit, cashing or collection (see the Bank's applicable account agreement for the definitions of "Item" and "Deposited Item");
 - (3) Give instructions to the Bank in writing (whether the instructions include the manual signature or a signature that purports to be the facsimile or other mechanical signature including a stamp of an Authorized Signer as the Customer's authorized signature without regard to when or by whom or by what means or in what ink color the signature may have been made or affixed), orally, by telephone or by any electronic means in regard to any Item and the transaction of any business relating to the Customer's account(s), agreements or services, and the Customer shall indemnify and hold the Bank harmless for acting in accordance with such instructions; and
 - (4) Delegate the person's authority to another person(s) or revoke such delegation, in a separate signed writing delivered to the Bank.
- C. If a code must be communicated to the Bank in order to authorize an Item, and the code is communicated, the Item will be binding on the Customer regardless of who communicated the code.**
- D. Each transaction described in this Certificate of Authority conducted by or on behalf of the Customer prior to delivery of this Certificate is in all respects ratified.**
- E. If the Customer is a tribal government or tribal government agency, the Customer waives sovereign immunity from suit with respect to the Customer's use of any Bank account, product or service referred to in this Certificate.**
- F. The information provided in this Application is correct and complete, each person who signs the "Certified/Agreed To" section of this Application and each person whose name appears in the "Authorized Signers-Signature Capture" section of this Application holds any position indicated, and the signature appearing opposite the person's name is authentic.**
- G. The Customer has approved this Certificate of Authority or granted each person who signs the "Certified/Agreed To" section of this Application the authority to do so on the Customer's behalf by:**
- (1) resolution, agreement or other legally sufficient action of the governing body of the Customer, if the Customer is not a trust or a sole proprietor;
 - (2) the signature of each of the Customer's trustee(s), if the Customer is a trust; or
 - (3) the signature of the Customer, if the Customer is a sole proprietor.



Business Account Application

Certified/Agreed ToOwner/Key Individual 1 Name
SADEGH AMINIANPosition/Title:
OWNER

Owner/Key Individual 1 Signature

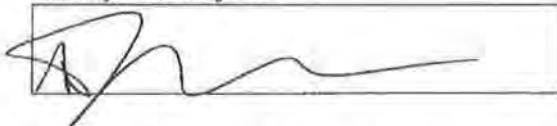
☒ Submit manually
☐ Signature not requiredDate:
01/26/2012

Owner/Key Individual 2 Name

PEGAH SADRHASHEMINEJAD

Position/Title:
PARTNER

Owner/Key Individual 2 Signature

☒ Submit manually
☐ Signature not requiredDate:
01/26/2012**Authorized Signers - Signature Capture**

Authorized Signer 1 Name

SADEGH AMINIAN

Position/Title:
OWNER

Authorized Signer 1 Signature

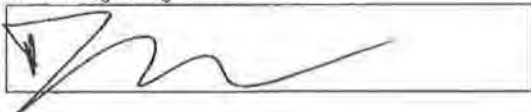
☒ Submit manually
☐ Signature not requiredDate:
01/26/2012

Authorized Signer 2 Name

PEGAH SADRHASHEMINEJAD

Position/Title:
PARTNER

Authorized Signer 2 Signature


☒ Submit manually
☐ Signature not requiredDate:
01/26/2012

Authorized Signer 3 Name

SEYED MOHSEN TORABI

Position/Title:
OWNER

Authorized Signer 3 Signature

☒ Submit manually
☐ Signature not requiredDate:
01/26/2012

Business Account Application

**WELLS
FARGO**

Bank Name:	Wells Fargo Bank, N.A.		Store Name:	West Hollywood	
Banker Name:	MARIE LOKMANYAN		Officer/Portfolio Number:	CN616	Date:
Banker Phone:	310/851-1140	Store Number:	04232	Banker AU:	0000378
				Banker MAC:	E2162-011

To help the government fight the funding of terrorism and money laundering activities, U.S. Federal law requires financial institutions to obtain, verify, and record information that identifies each person (individuals and businesses) who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

New Account Information

☒ New Deposit Account(s) Only ☐ New Deposit Account(s) and Business Credit Card

Account 1 Product Name

Expanded Business Services Package

COD:	Product:	Account Number:	Opening Deposit:	Type of Funds:
114	BDA	6505709052	\$100.00	CKS

Account 2 Product Name

Business High Yield Savings

COD:	Product:	Account Number:	Opening Deposit:	Type of Funds:
114	BDA	2018893525	\$100.00	CKS

New Account Kit:

Printed

Authorized Signers

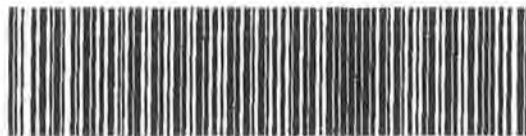
Business Name:

SAPENE LLC

Other Related Customer Name:

Authorized Signer Name(s):

PEGAN SADRIASHEMINIAD



Business Account Application

Checking/Savings Statement Mailing Information

Name(s) and Information Listed on Statement: SAPENE LLC	Statement Mailing Address: 1134 ALTA LOMA RD APT 303
	Address Line 2:
	City: WEST HOLLYWOOD State: CA
	ZIP/Postal Code: 90069-2433 Country: US

Business Information

Business Name: SAPENE LLC	Street Address: 1134 ALTA LOMA RD APT 303
Taxpayer Identification Number (TIN): 41-4319691	TIN Type: RTN
Business Type: Limited Liability Company	Address Line 2:
Business Sub-Type:	Address Line 3:
	City: WEST HOLLYWOOD State: CA
Date Originally Established: 07/10/2009	Current Ownership Since:
Annual Gross Sales: \$500,000.00	Year Sales Reported: 07/01/2010
Primary Financial Institution:	Number of Locations: 1
Sales Market: LOCAL	Number of Employees: 1
Primary State 1:	Fiscal Year End:
Primary State 2:	Business Phone: (412) 352-0363
Primary State 3:	Fax:
Primary Country 1:	Cellular Phone:
Primary Country 2:	Pager:
Primary Country 3:	e-Mail Address:
Industry: Agriculture, Forestry, Fishing and Hunting	Website:
Description of Business: AGRICULTURE PESTACIOS	
Major Suppliers/Customers: STRATUS GLOBAL	

Bank Use Only

Name/Entity Verification: Articles of Organization	Address Verification:	BACC Reference Number: 612BAC1313023
Document Filing Number/Description: 201201810164	Filing Country: US	Expiration Date:
Country of Registration: US	Filing State: CA	Check Reporting: NO RECORD
State of Registration: CA	Filing Date: 01/17/2012	
International Transactions: 		
Internet Gambling Business: No		



Business Account Application

Owner/Key Individual 1 Information

Customer Name: LEGAN SACHASHIEMINEJAD		Residence Address: 1134 ALTA LOMA RD APT 303	
Position/Title: FARTHER	Date of Birth: 02/10/1979	Address Line 2:	
Taxpayer Identification Number (TIN): 161-06-3885	TIN Type: SSN	Address Line 3:	
Primary ID Type: DLIC	Primary ID Description: S-362-680-007-108	City: WEST HOLLYWOOD	State: CA
Primary ID St/Ctry/Prov: CA	Primary ID Issue Date: 10/07/2010	Primary ID Expiration Date: 02/10/2016	ZIP/Postal Code: 90069-2433
Secondary ID Type: OTHER CC	Secondary ID Description: HSBC CC	Check Reporting: NO RECORD	
Secondary ID State/Country: CA	Secondary ID Issue Date: 01/01/2010	Secondary ID Expiration Date: 01/01/2013	
Country of Citizenship: TR	Permanently Resides in US: YES		

Certificate of Authority

Each person who signs the "Certified/Agreed To" section of this Application certifies that:

- A. The Customer's use of any Bank deposit account, product or service will confirm the Customer's receipt of, and agreement to be bound by, the Bank's applicable fee and information schedule and account agreement that includes the Arbitration Agreement under which any dispute between the Customer and the Bank relating to the Customer's use of any Bank deposit account, product or service will be decided in an arbitration proceeding before a neutral arbitrator as described in the Arbitration Agreement and not by a jury or court trial.**
- B. Each person who signs the "Certified/Agreed To" section of this Application or whose name, any applicable title and specimen signature appear in the "Authorized Signers - Signature Capture" section of this Application is authorized on such terms as the Bank may require to:**
- (1) Enter into, modify, terminate and otherwise in any manner act with respect to accounts at the Bank and agreements with the Bank or its affiliates for accounts and/or services offered by the Bank or its affiliates (other than letters of credit or loan agreements);
 - (2) Authorize (by signing or otherwise) the payment of Items from the Customer's account(s) listed on this Business Account Application (including without limitation any Item payable to (a) the individual order of the person who authorized the Item or (b) the Bank or any other person for the benefit of the person who authorized the Item) and the endorsement of Deposited Items for deposit, cashing or collection (see the Bank's applicable account agreement for the definitions of "Item" and "Deposited Item");
 - (3) Give instructions to the Bank in writing (whether the instructions include the manual signature or a signature that purports to be the facsimile or other mechanical signature including a stamp of an Authorized Signer as the Customer's authorized signature without regard to when or by whom or by what means or in what ink color the signature may have been made or affixed), orally, by telephone or by any electronic means in regard to any Item and the transaction of any business relating to the Customer's account(s), agreements or services, and the Customer shall indemnify and hold the Bank harmless for acting in accordance with such instructions; and
 - (4) Delegate the person's authority to another person(s) or revoke such delegation, in a separate signed writing delivered to the Bank.
- C. If a code must be communicated to the Bank in order to authorize an Item, and the code is communicated, the Item will be binding on the Customer regardless of who communicated the code.**
- D. Each transaction described in this Certificate of Authority conducted by or on behalf of the Customer prior to delivery of this Certificate is in all respects ratified.**
- E. If the Customer is a tribal government or tribal government agency, the Customer waives sovereign immunity from suit with respect to the Customer's use of any Bank account, product or service referred to in this Certificate.**
- F. The information provided in this Application is correct and complete, each person who signs the "Certified/Agreed To" section of this Application and each person whose name appears in the "Authorized Signers - Signature Capture" section of this Application holds any position indicated, and the signature appearing opposite the person's name is authentic.**
- G. The Customer has approved this Certificate of Authority or granted each person who signs the "Certified/Agreed To" section of this Application the authority to do so on the Customer's behalf by:**
- (1) resolution, agreement or other legally sufficient action of the governing body of the Customer, if the Customer is not a trust or a sole proprietor;
 - (2) the signature of each of the Customer's trustee(s), if the Customer is a trust; or
 - (3) the signature of the Customer, if the Customer is a sole proprietor.



Business Account Application

Certified/Agreed To

Owner/Key Individual 1 Name

PEGAH SADRHASHEMTNEJAD

Position/Title:

PARTNER

Owner/Key Individual 1 Signature




Submit manually



Signature not required

Date:

01/23/2012

Request for Taxpayer Identification Number and Certification

(Substitute Form W-9)

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
2. UNLESS I HAVE CHECKED ONE OF THE BOXES BELOW, I am not subject to backup withholding either because I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or the IRS has notified me that I am no longer subject to backup withholding (does not apply to real estate transactions, mortgage interest paid, the acquisition or abandonment of secured property, contributions to an Individual Retirement Arrangement (IRA), and payment other than interest and dividends).
3. I am a U.S. person (including a U.S. resident alien). ☐ I am subject to backup withholding ☐ I am exempt from backup withholding

Note: The Internal Revenue Service does not require your consent to any provision of this document other than the certifications required to avoid backup withholding.

Business Name:

SADENE, LLC

Taxpayer Identification Number (TIN):

45-4319695

TIN Certification Signature:




Submit manually



Signature not required

Date:

01/23/2012

Authorized Signers - Signature Capture

Authorized Signer 1 Name

PEGAH SADRHASHEMTNEJAD

Position/Title:

PARTNER

Authorized Signer 1 Signature



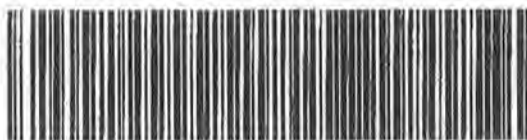

Submit manually



Signature not required

Date:

01/23/2012



Addendum To Certificate Of Authority

For Changes To Authorized Signers On Business Deposit Accounts

WELLS
FARGO

Host Status:

Host Update Successful

Bank Name:	Store Name:		
WELLS FARGO BANK, N.A.	CEDARS SINAI		
Banker Name:	Officer/Portfolio Number:	Date:	
NOONIK TARVERDIAN	C7627	10/01/2013	
Banker Phone:	Store Number:	Banker AU:	Banker MAC:
310/657-3951	04498	0000807	E2164-011

Use this Addendum when Authorized Signers are being added or deleted to a Certificate of Authority currently on file for a business customer and a new, signed Certificate of Authority has not been obtained.

Business/Account Information

Business Name:	COD:	Product:	Account Number:
SAPENE LLC	114	DDA	2018893525

Authorized Signers

Authorized Signer Name(s):	Relationship Status:		
PEGAH SADRHASHEMINEJAD	<input checked="" type="checkbox"/> Existing/Remaining	<input type="checkbox"/> New	<input type="checkbox"/> Delete
ALI SADR	<input type="checkbox"/> Existing/Remaining	<input checked="" type="checkbox"/> New	<input type="checkbox"/> Delete

Addendum to Certificate of Authority

Original Certificate of Authority Dated:	Addendum to Certificate of Authority Dated:
01/17/2012	10/01/2013

Each person signing in the "Certified/Agreed To" section below:

- directs the Bank that the additional Authorized Signers shall have all of the authority granted to the persons identified as Authorized Signers on the Certificate of Authority, including without limitation the authority to instruct the Bank in writing (whether the instructions include the manual signature or a signature that purports to be the facsimile or other mechanical signature including a stamp of an Authorized Signer as the Customer's authorized signature without regard to when or by whom or by what means or in what ink color the signature may have been made or affixed), orally, by telephone or by electronic means in regard to any item and the transaction of any business relating to the Customer's account(s), agreements or services;
- directs the Bank to discontinue acting on the instructions of any person who has been deleted as an Authorized Signer;
- acknowledges that these modifications become effective only after this Addendum has been received by the Bank and the Bank has had a reasonable opportunity to act on it; and
- certifies that the account owner has taken all action under its organizational documents, if any, including passage of resolutions by its board of directors, trustees, or other governing body, required to make these modifications and to authorize the undersigned to execute and deliver this Addendum.



BBG5351 (8-07 SVP)

© 2007 Wells Fargo Bank, N.A. All rights reserved.

2W02-000596850008-01

Page 1 of 2

Wells Fargo Confidential

Certified/Agreed To

Owner/Key Individual 1 Name

PEGAH SADRHASHEMINEJAD

Position/Title:

PARTNER

Owner/Key Individual 1 Signature

PEGAH SADRHASHEMINEJAD



☐ Submit manually

☐ Signature not required

Date:

10/01/2013

Signature Capture - New Authorized Signers

New Authorized Signer 1 Name


ALI SADR

Position/Title:

mgr partner

New Authorized Signer 1 Signature

ALI SADR



☐ Submit manually

☐ Signature not required

Date:

10/01/2013



Business Account Application



Bank Name: Wells Fargo Bank, N.A.		Store Name: MALIBU	
Banker Name: ARASH DOUNEL		Officer/Portfolio Number: A1054	Date: 09/07/2011
Banker Phone: 310/317-1740	Store Number: 04649	Banker AU: 0001902	Banker MAC: E2351-011

To help the government fight the funding of terrorism and money laundering activities, U.S. Federal law requires financial institutions to obtain, verify, and record information that identifies each person (individuals and businesses) who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

New Account Information

☒ New Deposit Account(s) Only ☐ New Deposit Account(s) and Business Credit Card

Account 1 Product Name Expanded Business Services Package				
COD:	Product:	Account Number:	Opening Deposit:	Type of Funds:
114	DDA	3803666647	\$9,900.00	INTX

Account 2 Product Name Business High Yield Savings				
COD:	Product:	Account Number:	Opening Deposit:	Type of Funds:
114	DDA	2504476439	\$100.00	INTX

New Account Kit: b20110404-0007329203
--

Authorized Signers

Business Name: SETOMA LLC	Other Related Customer Name:
Authorized Signer Name(s): SADEGH AMINIAN PEGAH SADRHASHEMINEJAD	SEYED MOHSEN TORABI



Business Account Application

Checking/Savings Statement Mailing Information

Name(s) and Information Listed on Statement: SETOMA LLC	Statement Mailing Address: 429 18TH ST	
	Address Line 2:	
	City: SANTA MONICA	State: CA
	ZIP/Postal Code: 90402-2429	Country: US

Business Information

Business Name: SETOMA LLC			Street Address: 429 18TH ST	
Taxpayer Identification Number (TIN): 45-3042794			Address Line 2:	
TIN Type: EIN			Address Line 3:	
Business Type: Limited Liability Company				
Business Sub-Type:			City: SANTA MONICA	State: CA
Non-Profit: No			ZIP/Postal Code: 90402-2429	Country: US
Date Originally Established: 08/17/2011	Current Ownership Since:	Number of Employees: 3		
Annual Gross Sales: \$1,000,000.00	Year Sales Reported: 08/01/2011	Fiscal Year End:	Business Phone: (818) 905-9105	Fax:
Primary Financial Institution:	Number of Locations: 1		Cellular Phone:	Pager:
Sales Market: LOCAL			e-Mail Address:	
Primary State 1:	Primary State 2:	Primary State 3:	Website:	
Primary Country 1:	Primary Country 2:	Primary Country 3:		
Industry: Agriculture, Forestry, Fishing and Hunting				
Description of Business: Pistachio Farming				
Major Suppliers/Customers:				

Bank Use Only

Name/Entity Verification: Articles of Organization			Address Verification:		BACC Reference Number: 611BAC2429250
Document Filing Number/Description: 201123010001	Filing Country: US	Filing State: CA	Filing Date: 08/17/2011	Expiration Date:	
Country of Registration: US	State of Registration: CA	International Transactions:	Check Reporting: NO RECORD		
Internet Gambling Business: No					



Business Account Application

Owner/Key Individual 1 Information

Customer Name: SADEGH AMINIAN	Primary ID Type: DLIC	Primary ID Description: C0033250	
Position/Title: OWNER	Primary ID St/Ctry/Prov: CA	Primary ID Issue Date: 12/01/2009	Primary ID Expiration Date: 12/09/2014
Check Reporting: NO RECORD	Secondary ID Type: OTHR DC	Secondary ID Description: WF VISA	
	Secondary ID State/Country:	Secondary ID Issue Date:	Secondary ID Expiration Date: 07/01/2012

Owner/Key Individual 2 Information

Customer Name: SEYED MOHSEN TORABI	Primary ID Type: ALID PR	Primary ID Description: 061-381-569	
Position/Title: OWNER	Primary ID St/Ctry/Prov:	Primary ID Issue Date: 03/10/2011	Primary ID Expiration Date: 03/10/2013
Check Reporting: NO RECORD	Secondary ID Type: OTHR CC	Secondary ID Description: CITI CC	
	Secondary ID State/Country:	Secondary ID Issue Date: 10/01/2010	Secondary ID Expiration Date: 12/01/2014

Owner/Key Individual 3 Information

Customer Name: PEGAH SADRHASHEMINEJAD	Primary ID Type: DLIC	Primary ID Description: S-362-680-007-108	
Position/Title: PARTNER	Primary ID St/Ctry/Prov: MD	Primary ID Issue Date: 10/07/2010	Primary ID Expiration Date: 02/10/2016
Check Reporting: NO RECORD	Secondary ID Type: OTHR CC	Secondary ID Description: HSBC CC	
	Secondary ID State/Country:	Secondary ID Issue Date: 01/01/2010	Secondary ID Expiration Date: 01/01/2013



Certificate of Authority

Each person who signs the "Certified/Agreed To" section of this Application certifies that:

- A. The Customer's use of any Bank deposit account, product or service will confirm the Customer's receipt of, and agreement to be bound by, the Bank's applicable fee and information schedule and account agreement that includes the Arbitration Agreement under which any dispute between the Customer and the Bank relating to the Customer's use of any Bank deposit account, product or service will be decided in an arbitration proceeding before a neutral arbitrator as described in the Arbitration Agreement and not by a jury or court trial.**
- B. Each person who signs the "Certified/Agreed To" section of this Application or whose name, any applicable title and specimen signature appear in the "Authorized Signers - Signature Capture" section of this Application is authorized on such terms as the Bank may require to:**
- (1) Enter into, modify, terminate and otherwise in any manner act with respect to accounts at the Bank and agreements with the Bank or its affiliates for accounts and/or services offered by the Bank or its affiliates (other than letters of credit or loan agreements);
 - (2) Authorize (by signing or otherwise) the payment of Items from the Customer's account(s) listed on this Business Account Application (including without limitation any Item payable to (a) the individual order of the person who authorized the Item or (b) the Bank or any other person for the benefit of the person who authorized the Item) and the endorsement of Deposited Items for deposit, cashing or collection (see the Bank's applicable account agreement for the definitions of "Item" and "Deposited Item");
 - (3) Give instructions to the Bank in writing (whether the instructions include the manual signature or a signature that purports to be the facsimile or other mechanical signature including a stamp of an Authorized Signer as the Customer's authorized signature without regard to when or by whom or by what means or in what ink color the signature may have been made or affixed), orally, by telephone or by any electronic means in regard to any Item and the transaction of any business relating to the Customer's account(s), agreements or services, and the Customer shall indemnify and hold the Bank harmless for acting in accordance with such instructions; and
 - (4) Delegate the person's authority to another person(s) or revoke such delegation, in a separate signed writing delivered to the Bank.
- C. If a code must be communicated to the Bank in order to authorize an Item, and the code is communicated, the Item will be binding on the Customer regardless of who communicated the code.**
- D. Each transaction described in this Certificate of Authority conducted by or on behalf of the Customer prior to delivery of this Certificate is in all respects ratified.**
- E. If the Customer is a tribal government or tribal government agency, the Customer waives sovereign immunity from suit with respect to the Customer's use of any Bank account, product or service referred to in this Certificate.**
- F. The information provided in this Application is correct and complete, each person who signs the "Certified/Agreed To" section of this Application and each person whose name appears in the "Authorized Signers-Signature Capture" section of this Application holds any position indicated, and the signature appearing opposite the person's name is authentic.**
- G. The Customer has approved this Certificate of Authority or granted each person who signs the "Certified/Agreed To" section of this Application the authority to do so on the Customer's behalf by:**
- (1) resolution, agreement or other legally sufficient action of the governing body of the Customer, if the Customer is not a trust or a sole proprietor;
 - (2) the signature of each of the Customer's trustee(s), if the Customer is a trust; or
 - (3) the signature of the Customer, if the Customer is a sole proprietor.


Certified/Agreed To

Owner/Key Individual 1 Name
SADEGH AMINIAN

Position/Title:
OWNER

Owner/Key Individual 1 Signature

SADEGH AMINIAN



- ☐ Submit manually
☐ Signature not required

Date:
09/07/2011

Owner/Key Individual 2 Name
SEYED MOHSEN TORABI

Position/Title:
OWNER

Owner/Key Individual 2 Signature

SEYED MOHSEN TORABI



- ☐ Submit manually
☐ Signature not required

Date:
09/07/2011



Business Account Application

Request for Taxpayer Identification Number and Certification

(Substitute Form W-9)

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
2. UNLESS I HAVE CHECKED ONE OF THE BOXES BELOW, I am not subject to backup withholding either because I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or the IRS has notified me that I am no longer subject to backup withholding (does not apply to real estate transactions, mortgage interest paid, the acquisition or abandonment of secured property, contributions to an Individual Retirement Arrangement (IRA), and payment other than interest and dividends).
3. I am a U.S. person (including a U.S. resident alien). ☐ I am subject to backup withholding ☐ I am exempt from backup withholding

Note: The Internal Revenue Service does not require your consent to any provision of this document other than the certifications required to avoid backup withholding.

Business Name:

SETOMA LLC

Taxpayer Identification Number (TIN):

45-3042794

TIN Certification Signature:

SADEGH AMINIAN


☐ Submit manually☐ Signature not required

Date:

09/07/2011

Authorized Signers - Signature Capture

Authorized Signer 1 Name

SADEGH AMINIAN

Position/Title:

OWNER

Authorized Signer 1 Signature

SADEGH AMINIAN


☐ Submit manually☐ Signature not required

Date:

09/07/2011

Authorized Signer 2 Name


SEYED MOHSEN TORABI

Position/Title:

OWNER

Authorized Signer 2 Signature

SEYED MOHSEN TORABI


☐ Submit manually☐ Signature not required

Date:

09/07/2011

Authorized Signer 3 Name

PEGAH SADRHASHEMINEJAD

Position/Title:

PARTNER

Authorized Signer 3 Signature

PEGAH SADRHASHEMINEJAD


☐ Submit manually☐ Signature not required

Date:

09/07/2011



Business Account Application



Bank Name: WELLS FARGO BANK, N.A.		Store Name: CEDARS SINAI	
Banker Name: MARIE LOKMANYAN		Officer/Portfolio Number: CN616	Date: 12/14/2012
Banker Phone: 310/657-3951	Store Number: 04498	Banker AU: 0000807	Banker MAC: E2164-011

To help the government fight the funding of terrorism and money laundering activities, U.S. Federal law requires financial institutions to obtain, verify, and record information that identifies each person (individuals and businesses) who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

New Account Information

☒ New Deposit Account(s) Only ☐ New Deposit Account(s) and Business Credit Card

Account 1 Product Name: Wells Fargo Business High Yield Savings				
COD: 114	Product: DDA	Account Number: 9221977151	Opening Deposit: \$100.00	Type of Funds: CASH
Account 2 Product Name: Gold Business Services Package				
COD: 114	Product: DDA	Account Number: 9016420896	Opening Deposit: \$100.00	Type of Funds: CKS

New Account Kit: Printed

Related Customer Information

Customer 1 Name: SLAG CONST LLC	Account Relationship: Sole Owner
Enterprise Customer Number (ECN): 324546792249215	
Customer 2 Name: PEGAH SADRHASHEMINEJAD	Account Relationship: Signer
Enterprise Customer Number (ECN): 228421802054710	



Business Account Application

Checking/Savings Statement Mailing Information

Name(s) and Information Listed on Statement: SLAG CONST LLC	Statement Mailing Address: 1134 ALTA LOMA RD APT 303	
	Address Line 2:	
	City: WEST HOLLYWOOD	State: CA
	ZIP/Postal Code: 90069-2433	Country: US

Customer 1 Information

Customer Name: SLAG CONST LLC		Street Address: 1134 ALTA LOMA RD APT 303	
Account Relationship: Sole Owner		Address Line 2:	
Taxpayer Identification Number (TIN): 45-4292603		Address Line 3:	
TIN Type: EIN			
Business Type: Limited Liability Company		City: WEST HOLLYWOOD	State: CA
Business Sub-Type/Tax Classification: S Corporation		ZIP/Postal Code: 90069-2433	Country: US
Non-Profit: No			
Date Originally Established: 06/04/2012	Current Ownership Since: 06/04/2012	Number of Employees: 1	Business Phone: 412/352-0363
Annual Gross Sales: \$100,000.00		Year Sales Reported: 06/04/2012	Fax:
Fiscal Year End: 		Cellular Phone: 	Pager:
Primary Financial Institution: 		e-Mail Address: 	
Number of Locations: 1			
Primary State 1: 	Primary State 2: 	Primary State 3: 	Website:
Primary Country 1: 	Primary Country 2: 	Primary Country 3: 	Sales Market: LOCAL
Industry: Construction			
Description of Business: 			
Major Suppliers/Customers: 			

Bank Use Only

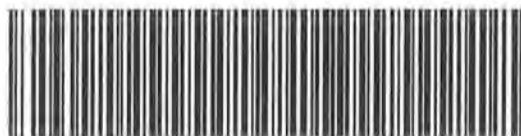
Name/Entity Verification: Secretary of State		Address Verification:		BACC Reference Number: 612BAC2852349
Document Filing Number/Description: 201201710043	Filing Country: US	Filing State: CA	Filing Date: 06/04/2012	Expiration Date:
Country of Registration: US	State of Registration: CA	International Transactions: 		Check Reporting: NO RECORD
Customer 1 Name: SLAG CONST LLC			Internet Gambling Business?: No	



Business Account Application

Owner/Key Individual 1 Information

Customer Name: PEGAH SADRHASHEMINEJAD			Residence Address: 1134 ALTA LOMA RD APT 303	
Position/Title: PARTNER	Date of Birth: 02/10/1979	Enterprise Customer Number (ECN): 228421802054710	Address Line 2:	
Taxpayer Identification Number (TIN): 141-06-3068	TIN Type: SSN	Address Line 3:		
Primary ID Type: DLIC	Primary ID Description: S-362-680-007-108	City: WEST HOLLYWOOD	State: CA	
Primary ID St/Ctry/Prov: MD	Primary ID Issue Date: 10/07/2010	Primary ID Expiration Date: 02/10/2016	ZIP/Postal Code: 90069-2433	Country: US
Secondary ID Type: OTHR CC	Secondary ID Description: HSBC CC	Check Reporting: NO RECORD		
Secondary ID State/Country:	Secondary ID Issue Date: 01/01/2010	Secondary ID Expiration Date: 01/01/2014		
Country of Citizenship: IR	Permanently Resides in US: YES			



Certificate of Authority

Each person who signs the "Certified/Agreed To" section of this Application certifies that:

- A. The Customer's use of any Bank deposit account, product or service will confirm the Customer's receipt of, and agreement to be bound by, the Bank's applicable fee and information schedule and account agreement that includes the Arbitration Agreement under which any dispute between the Customer and the Bank relating to the Customer's use of any Bank deposit account, product or service will be decided in an arbitration proceeding before a neutral arbitrator as described in the Arbitration Agreement and not by a jury or court trial.**
- B. Each person who signs the "Certified/Agreed To" section of this Application or whose name, any applicable title and specimen signature appear in the "Authorized Signers - Signature Capture" section of this Application is authorized on such terms as the Bank may require to:
- (1) Enter into, modify, terminate and otherwise in any manner act with respect to accounts at the Bank and agreements with the Bank or its affiliates for accounts and/or services offered by the Bank or its affiliates (other than letters of credit or loan agreements);
 - (2) Authorize (by signing or otherwise) the payment of Items from the Customer's account(s) listed on this Business Account Application (including without limitation any Item payable to (a) the individual order of the person who authorized the Item or (b) the Bank or any other person for the benefit of the person who authorized the Item) and the endorsement of Deposited Items for deposit, cashing or collection (see the Bank's applicable account agreement for the definitions of "Item" and "Deposited Item");
 - (3) Give instructions to the Bank in writing (whether the instructions include the manual signature or a signature that purports to be the facsimile or other mechanical signature including a stamp of an Authorized Signer as the Customer's authorized signature without regard to when or by whom or by what means or in what ink color the signature may have been made or affixed), orally, by telephone or by any electronic means in regard to any Item and the transaction of any business relating to the Customer's account(s), agreements or services, and the Customer shall indemnify and hold the Bank harmless for acting in accordance with such instructions; and
 - (4) Delegate the person's authority to another person(s) or revoke such delegation, in a separate signed writing delivered to the Bank.
- C. If a code must be communicated to the Bank in order to authorize an Item, and the code is communicated, the Item will be binding on the Customer regardless of who communicated the code.
- D. Each transaction described in this Certificate of Authority conducted by or on behalf of the Customer prior to delivery of this Certificate is in all respects ratified.
- E. If the Customer is a tribal government or tribal government agency, the Customer waives sovereign immunity from suit with respect to the Customer's use of any Bank account, product or service referred to in this Certificate.
- F. The information provided in this Application is correct and complete, each person who signs the "Certified/Agreed To" section of this Application and each person whose name appears in the "Authorized Signers-Signature Capture" section of this Application holds any position indicated, and the signature appearing opposite the person's name is authentic.
- G. The Customer has approved this Certificate of Authority or granted each person who signs the "Certified/Agreed To" section of this Application the authority to do so on the Customer's behalf by:
- (1) resolution, agreement or other legally sufficient action of the governing body of the Customer, if the Customer is not a trust or a sole proprietor;
 - (2) the signature of each of the Customer's trustee(s), if the Customer is a trust; or
 - (3) the signature of the Customer, if the Customer is a sole proprietor.

Certified/Agreed To

Owner/Key Individual 1 Name

PEGAH SADRHASHEMINEJAD

Position/Title:

PARTNER

Owner/Key Individual 1 Signature



Submit manually



Signature not required

Date:

12/14/2012



Business Account Application

Request for Taxpayer Identification Number and Certification

(Substitute Form W-9)

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
2. UNLESS I HAVE CHECKED ONE OF THE BOXES BELOW, I am not subject to backup withholding either because I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or the IRS has notified me that I am no longer subject to backup withholding (does not apply to real estate transactions, mortgage interest paid, the acquisition or abandonment of secured property, contributions to an Individual Retirement Arrangement (IRA), and payment other than interest and dividends).
3. I am a U.S. citizen or other U.S. person. ☐ I am subject to backup withholding ☐ I am exempt from backup withholding

Note: The Internal Revenue Service does not require your consent to any provision of this document other than the certifications required to avoid backup withholding.

Tax Responsible Customer Name:

SLAG CONST LLC

Taxpayer Identification Number (TIN):

45-4292603

TIN Certification Signature:

- ☒ Submit manually
☐ Signature not required

Date:

Authorized Signers - Signature Capture

Authorized Signer 1 Name

PEGAH SADRHASHEMINEJAD

Position/Title:

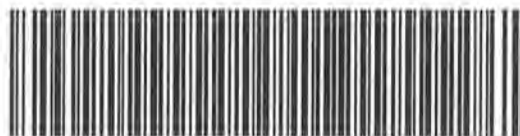
PARTNER

Authorized Signer 1 Signature

- ☒ Submit manually
☐ Signature not required

Date:

12/14/2012



Consumer Account Application

**WELLS
FARGO**

 Bank Name:
WELLS FARGO BANK, N.A.

 Banker Name:
MARIE LOKMANYAN

 Banker Phone:
310/657-3951

 Store Number:
04498

 Store Name:
CEDARS SINAI

 Officer/Portfolio Number:
CN616

 Banker AU:
0000807

 Date:
05/22/2012

 Banker MAC:
E2164-011

To help the government fight the funding of terrorism and money laundering activities, U.S. Federal law requires financial institutions to obtain, verify, and record information that identifies each person (individuals and businesses) who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

New Account Information

Product Name:	Minor:	COID:	Product:	Account Number:
PMA Premier Checking		114	CDA	15836451213

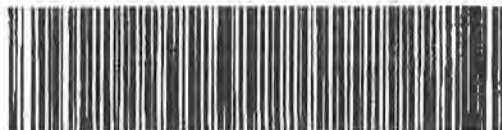
 New Account Kit:
Printed

Related Customers

Customer Name:	Account Relationship:
PEGAN SADRHASHEMINEJAD	Sole Owner

Checking/Savings Statement Mailing Information

Customer(s) Listed on Statement:	Statement Mailing Address:	
PEGAN SADRHASHEMINEJAD	1134 ALTA LOMA RD APT 303	
	Address Line 2:	
	City:	State:
	WEST HOLLYWOOD	CA
	ZIP/Postal Code:	Country:
	90069-2433	US



Consumer Account Application

Customer 1 Information

Customer Name: PEGAN SARRHASHEMINEJAD		Street Address: 1134 ALTA LOMA RD APT 303	
Account Relationship: Sole Owner		Address Line 2:	
Taxpayer Identification Number (TIN): 41-06-3068		TIN Type: SSN	Date of Birth: 02/10/1979
Primary ID Type: CC	Primary ID Description: S-362-680-007-108	City: WEST HOLLYWOOD	
Primary ID State/Prov: MT	Primary ID Issue Date: 10/07/2010	Primary ID Expiration Date: 02/10/2016	State: CA
Secondary ID Type: OTHER CC	Secondary ID Description: HSBC CC	ZIP/Postal Code: 90069-2433	Country: US
Secondary ID State/Country:	Secondary ID Issue Date: 01/01/2010	Secondary ID Expiration Date: 01/01/2014	Time at this address: 12 Year(s) 4 Month(s)
Home Phone: 412/352-0363	Business Phone: 412/352-0363	Directional Address: (Document when no physical residence, business or alternate street address.)	
Current Employer: SETH SLAC CONST. LLC	Previous Street Address:		
Check Reporting: NO RECORD	City: State:		
Country of Citizenship: IR	ZIP/Postal Code: Country: Time at this address: Year(s) Month(s)		
Permanently Resides In US: YES			

Request for Taxpayer Identification Number and Certification

(Substitute Form W-9)

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
- UNLESS I HAVE CHECKED ONE OF THE BOXES BELOW, I am not subject to backup withholding either because I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or the IRS has notified me that I am no longer subject to backup withholding (does not apply to real estate transactions, mortgage interest paid, the acquisition or abandonment of secured property, contributions to an Individual Retirement Arrangement (IRA), and payment other than interest and dividends).
- I am a U.S. citizen or other U.S. person. ☐ I am subject to backup withholding ☐ I am exempt from backup withholding

Tax Responsible Customer Name:

PEGAN SARRHASHEMINEJAD

Taxpayer Identification Number (TIN):

41-06-3068

TIN Certification Signature


☒ Submit manually☐ Signature not required

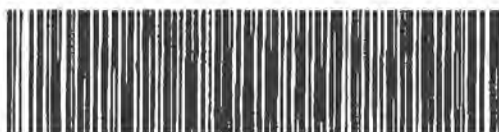
Date:

05/24/2012

Customer Signatures

Everything I have stated in this application is correct. You are authorized to make any inquiries that you consider appropriate to determine if you should open or maintain the account. This may include ordering a credit report or other report (i.e. information from any motor vehicle department or other state agency) on me. I have received a copy of the applicable account agreement, the privacy policy, and the Direct Deposit Advance Service Agreement and Product Guide* (as each may be amended from time to time) and agree to be bound by their terms. I also agree to the terms of the dispute resolution program described in the foregoing agreements. Under the dispute resolution program, our disputes will be decided before one or more neutral persons in an arbitration proceeding and not by a jury trial or a trial before a judge.

*The Direct Deposit Advance service is not currently available in all states.



Consumer Account Application

Customer 1 Name

PEGAH SAURHASEMINEJAD

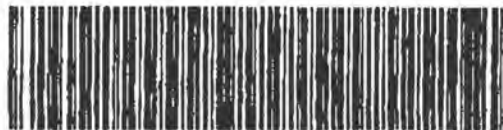
Customer 1 Signature



☒ Submit manually
☐ Signature not required

Date:

05/22/2012



Consumer Account Application



Bank Name: WELLS FARGO BANK, N.A.		Store Name: BETHESDA NORTH	
Banker Name: TRENDY INGRAM		Officer/Portfolio Number: E3843	Date: 03/09/2012
Banker Phone: 301/907-2030	Store Number: 08351	Banker AU: 0067111	Banker MAC: R1006-010

To help the government fight the funding of terrorism and money laundering activities, U.S. Federal law requires financial institutions to obtain, verify, and record information that identifies each person (individuals and businesses) who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

New Account Information

Product Name: PMA Premier Checking	Minor: 	COD: 336	Product: DDA	Account Number: 1891892364
New Account Kit: c20110404-0027587438				

Related Customers

Customer Name: SHOKOUH AZAM SHAFIEE AZAD	Account Relationship: Sole Owner
---	-------------------------------------

Checking/Savings Statement Mailing Information

Customer(s) Listed on Statement: SHOKOUH AZAM SHAFIEE AZAD	Statement Mailing Address: 7117 NATELLI WOODS LN	
	Address Line 2: 	
	City: BETHESDA	State: MD
	ZIP/Postal Code: 20817-3927	Country: US



Consumer Account Application

Customer 1 Information

Customer Name: SHOKOUH AZAM SHAFIEE AZAD		Street Address: 7117 NATELLI WOODS LN	
Account Relationship: Sole Owner		Address Line 2:	
Taxpayer Identification Number (TIN): 220-55-3780		TIN Type: SSN	Date of Birth: 05/10/1958
Address Line 3:			
Primary ID Type: DLIC	Primary ID Description: S-123-765-079-356	City: BETHESDA	State: MD
Primary ID St/Ctry/Prov: MD	Primary ID Issue Date: 03/09/2012	Primary ID Expiration Date: 05/10/2017	ZIP/Postal Code: 20817-3927
		Country: US	Time at this address: Year(s) Month(s)
Secondary ID Type: OTHR DC	Secondary ID Description: WF VISA	Directional Address: (Document when no physical residence, business or alternate street address.)	
Secondary ID State/Country:	Secondary ID Issue Date:	Secondary ID Expiration Date: 02/01/2015	
Home Phone: 301/469-6245	Business Phone:	Previous Street Address:	
Current Employer: STUDENT		City:	State:
Check Reporting: NO RECORD		ZIP/Postal Code:	Country:
			Time at this address: Year(s) Month(s)
Country of Citizenship: US			

Request for Taxpayer Identification Number and Certification

(Substitute Form W-9)

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
- UNLESS I HAVE CHECKED ONE OF THE BOXES BELOW, I am not subject to backup withholding either because I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or the IRS has notified me that I am no longer subject to backup withholding (does not apply to real estate transactions, mortgage interest paid, the acquisition or abandonment of secured property, contributions to an Individual Retirement Arrangement (IRA), and payment other than interest and dividends).
- I am a U.S. person (including a U.S. resident alien), ☐ I am subject to backup withholding ☐ I am exempt from backup withholding

Tax Responsible Customer Name:

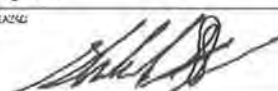
SHOKOUH AZAM SHAFIEE AZAD

Taxpayer Identification Number (TIN):

220-55-3780

TIN Certification Signature

SHOKOUH AZAM SHAFIEE AZAD


☐ Submit manually☐ Signature not required

Date:

03/09/2012

Customer Signatures

Everything I have stated in this application is correct. You are authorized to make any inquiries that you consider appropriate to determine if you should open the account. This may include obtaining a credit report or other report (i.e. information from any motor vehicle department or other state agency) on me. I have received a copy of the applicable account agreement and privacy brochure and agree to be bound by them, including the terms of the Direct Deposit Advance® service described in the Service Agreement and Product Guide and any amendment or addendum (Direct Deposit Advance service currently not available in all states). I also agree to the terms of the dispute resolution program described in the account agreement and the Direct Deposit Advance Service Agreement and Product Guide. Under this program our disputes will be decided before one or more neutral persons in an arbitration proceeding and not by a jury trial or a trial before a judge.



Consumer Account Application

Customer 1 Name

SHOKOUH AZAM SHAFIEE AZAD

Customer 1 Signature

SHOKOUH AZAM SHAFIEE AZAD

☐

Submit manually

☐

Signature not required

Date:

03/09/2012



Business Direct Credit Application

Agreement & Personal Guarantee**WELLS
FARGO**

Banker Name:	Officer/Portfolio Number:	Date:
NOONIK TARVERDIAN	C7627	10/01/2013
Banker Phone:	Store Number:	Banker AU:
310/657-3951	22164	0000807
		Banker MAC:
		E2164-011

Business/Application Information

Business Name:	Application ID:
SAPENE LLC	SVPP000004694760
Credit Application for:	Amount Requested:
Wells Fargo Business Platinum card	\$50,000

Acknowledgment & Customer Signature:

By signing below, I certify that I am an owner, partner, member, shareholder, director, and/or officer of the business named above ("Applicant"). I am authorized to submit this application on behalf of the "Applicant" and that all information and documents provided in connection with this application, including federal and state income tax returns (if any), are true, correct and complete. I further certify that this credit request is for my business only, and that all proceeds will be used solely for business or commercial purposes. I authorize Wells Fargo Bank, N.A. ("Bank") to obtain balance and payoff information and requires verification of payoff on all accounts requiring payoff as a condition of approving this application and to obtain at any time consumer and business reports from and to report credit information to others, including the Internal Revenue Service and state taxing authorities, about me and my business, both in connection with this application as well as any review, extension or renewal of the credit granted pursuant to this application. I also authorize Bank to use such information and to share with its affiliates in order to determine whether the business is qualified for other products and services offered by Bank and its affiliates. I agree to notify Bank promptly of any material change in such information. I acknowledge that (i) this application is subject to final approval of the Applicant and its owners, and that (ii) additional information (e.g., financial statements, tax returns and /or IRS Form 4506-T Request For Transcript of Tax Return) may be required in order for Bank to make a final credit decision. A facsimile of my signature, in any capacity, may be used as evidence of the Applicant's acceptance of these agreements. Note: Except in Arizona, if the business owner is married, a spouse's signature is not required unless he or she is the co-owner of the business. **If the Applicant is a legal entity, all owners listed on this application are asked to sign below and include their titles.**

NON-PROFIT NOTICE AND DISCLAIMER: Not-for-profit organizations are not eligible for the Secured BusinessLine line of credit. If the applicant is a not-for-profit organization recognized by and in good standing with the Internal Revenue Service, the personal guaranty of the signer is not required, and the personal guaranty paragraph below shall have no force or effect.

For Wells Fargo BusinessLine, Wells Fargo Secured BusinessLine, Wells Fargo Equipment Express, Wells Fargo Business Platinum card, Wells Fargo Business Secured card, Wells Fargo Small Business Advantage Line of Credit and Wells Fargo BusinessLoan applicants: By signing below, I agree on behalf of the Applicant to be bound by the terms of the Customer Agreement, Wells Fargo Business Lending Confirmation Letter (where applicable) and other written documentation that will be sent to Applicant and to pay Bank's costs and attorneys' fees in enforcing the Customer Agreement and other written documentation. I further agree that use of any feature of the BusinessLine line of credit, Equipment Express loan, Wells Fargo Business Platinum card, Wells Fargo Business Secured card, Wells Fargo Small Business Advantage line of credit or Wells Fargo BusinessLoan term loan may be used as evidence of the foregoing authorizations, acceptances, and agreements. For the Equipment Express loan, interest charges will start from the date we issue the check to fund the loan(s). For unsecured Wells Fargo Business Platinum card, Wells Fargo BusinessLine, Wells Fargo Equipment Express, Wells Fargo Small Business Advantage Line of Credit and Wells Fargo BusinessLoan, if approved, I agree to accept the actual credit amount granted which may be less than the preferred amount. If the actual credit granted is less than the preferred amount, individual credit lines will be reduced proportionately. For the Wells Fargo Secured BusinessLine and Wells Fargo Business Secured card, I acknowledge that it will be a condition for granting the credit facility that it be secured by an eligible CD/Savings account (Wells Fargo Secured BusinessLine) or deposit account (Wells Fargo Business Secured Card) maintained with Bank in an amount equal to or greater than the actual credit granted. For the Wells Fargo BusinessLoan term loan, I authorize Wells Fargo to distribute the loan proceeds electronically into credit and/or deposit accounts I designate, or to distribute the proceeds via check to the address listed herein. I acknowledge that the check will be valid for only 30 days after issuance, and agree that the Applicant will be held responsible for funds that are received, regardless of who deposits or negotiates the check.

By signing below, I also, **in my individual capacity** (even though I may place a title or other designation next to my signature), jointly and severally unconditionally guarantee and promise to pay to Bank all indebtedness of the Applicant at any time arising under or relating to any credit requested through this application, as well as any extensions, increases or renewals of that indebtedness. As guarantor, I waive (i) any requirement that Bank (A) proceed against Applicant or any other person; (B) marshal assets or proceed against or exhaust any security held from any Applicant or any other person; (C) give notice of the terms, time and place of any public or private sale or other disposition of personal property security held from any of the Applicants or any other person; (D) take any other action or pursue any other remedy in Bank's power; or (E) make any presentment, demand, protest, notice of protest, and notice of non-payment hereunder or in connection with any obligations or evidences of indebtedness held by Bank as security for or which constitute in whole or in part the Indebtedness guaranteed hereunder; (ii) any defense arising by reason of any defense of the Applicant or other guarantor; and (iii) the right to require Bank to proceed against the Applicant or any other guarantor, to pursue any remedy in connection with the guaranteed indebtedness, or to notify guarantor of any additional indebtedness incurred by the Applicant, or of any changes in the Applicant's financial condition. I also authorize Bank, without notice or prior consent, to (i) extend, modify, compromise, accelerate, renew, increase

Manual Submission Instructions:
Fax all pages of the signed form to
Business Direct at 1-866-814-7729.
Scanner enabled store: should scan



Acknowledgment & Customer Signature (Continued):

or otherwise change the terms of the guaranteed indebtedness; (ii) proceed against one or more guarantors without proceeding against the Applicant or another guarantor; and (iii) release or substitute any party to the indebtedness or this guaranty; and (iv) take and hold security for the payment of this Guaranty or the Indebtedness of Applicant or any portion thereof, and exchange, enforce, waive, subordinate or release any such security; (c) apply such security and direct the order or manner of sale thereof, including without limitation, a non-judicial sale permitted by the terms of the controlling security agreement, as Bank in its discretion may determine, and Guarantor hereby waives any provision of law regarding application of payments which specifies otherwise. I agree (i) I will pay Bank's costs and attorneys' fees in enforcing this guaranty (ii) this guaranty will be governed by South Dakota law; and (iii) this guaranty shall benefit Bank and its successors and assigns; and (iv) an electronic facsimile of my signature, in any capacity, may be used as evidence of my agreement to the terms of this guaranty.

Optional Credit Protection Program: This program will cancel debt on your *BusinessLine* and/or *Secured BusinessLine* if you are unable to work due to a major event as described in the Terms and Conditions for the Credit Protection program that will be provided to you. The debt cancellation will be a fixed benefit payment equal to 5% of the balance plus the Credit Protection service fee on the statement immediately following the covered event. It is not a waiver of any amounts due on your credit account(s). You agree to pay the monthly Credit Protection fees (\$0.35/\$100 of average daily balance) as charged based on the average daily balance for the Primary Account and all Linked accounts. If Credit Protection fees are not paid each month, fees will become part of the account balance and interest will accrue. In order to be eligible for debt cancellation, you must have met the eligibility requirements and be enrolled for 30 days before the benefit amount is requested and approved. Once you have enrolled, you will receive a complete Terms and Conditions for the Credit Protection Program. Please read it and keep for future reference.

Telephone Monitoring And Contacting You: From time to time Bank may monitor and record telephone calls regarding your Account to assure the quality of our service. You agree, in order for Bank to service the Account or to collect any amounts you may owe, that we may from time to time make calls and send text messages to you, using prerecorded/artificial voice messages and/or through the use of an automatic dialing device, at any telephone number associated with your account, including mobile telephone numbers that could result in charges to you. You also expressly consent to Bank sending email messages regarding your Account to your email address.


New Account Identification Requirements: To help the government fight the funding of terrorism and money laundering activities, U.S. Federal law requires financial institutions to obtain, verify, and record information that identifies each person (individuals and businesses) who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Owner/Guarantor/Signer 1 Name
PEGAH SADRHASHEMINEJAD

Position/Title:
partner

Customer Number (ECN):
228421802054710

Owner/Guarantor/Signer 1 Signature



- ☐ Submit manually
☐ Signature not required


Date:
10/01/2013

Owner/Guarantor/Signer 2 Name
ALI SADR

Position/Title:
partner

Customer Number (ECN):
700499054641634

Owner/Guarantor/Signer 2 Signature



- ☐ Submit manually
☐ Signature not required

Date:
10/01/2013

Manual Submission Instructions:
Fax all pages of the signed form to
Business Direct at 1-866-814-7729.
Scanner enabled store: should scan



2W02-000596865296-02